TESTING THE MALICIOUS USB ANECDOTE

BY

MATTHEW TISCHER

THESIS

Submitted in partial fulfillment of the requirements
for the degree of Master of Science in Electrical and Computer Engineering
in the Graduate College of the
University of Illinois at Urbana-Champaign, 2015

Urbana, Illinois

Adviser:

Associate Professor Michael Bailey

ABSTRACT

In today's computer security climate, attacks against computers are becoming increasingly sophisticated and cheaper to execute. In this thesis, we present the results of a study conducted on the University of Illinois campus to determine the effectiveness of dropping 297 "infected" USB flash drives in a public place as an attack vector. A self-report survey given to 71 individuals highlights some of the psychological processes that motivate people to plug in the flash drives. We find that this type of attack is generally effective and relatively insensitive to its precise environmental configuration. Generally, participants expressed desire to return the flash drives to their owners, although our data shows that they also explored the contents of the flash drives on occasion.

To my parents, for their love and support.

ACKNOWLEDGMENTS

I would like to offer my special thanks to Professor Michael Bailey for guiding this work from start to finish. I also greatly appreciate the essential assistance given by Sam Foster, Sunny Duan, Alec Mori, and Troy Chmieleski.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1.1 Introduction

While much recent attention has been directed towards technical exploits, such as Heartbleed [1], VENOM [2] or the Shellshock vulnerability [3], we direct our attention in this thesis to another relevant threat: social engineering. Social engineering attacks have significant financial cost [4], outweighing stolen devices, malware, and botnets [5]. They are also common; 42% of surveyed companies in Ponemon's 2013 Cost of Cyber Crime Study have experienced a social engineering attack during the four-week benchmark period [5].

In this thesis, we investigate a classic anecdote, in which an attacker infects a set of USB flash drives with malware and drops them into the parking lot of an organization that they wish to compromise. Legitimate users in the organization see the flash drives, pick them up, and insert them into their computers, allowing the attacker an opportunity to run malware on the flash drives on the computers and compromise the organization. Recent attacks, such as Stuxnet [6] and BadUSB [7] underscore the risk that unknown flash drives present to organizations.

We seek to answer three main questions in this work:

1. Is this attack viable in the real world? In other words, do people actually pick up the USB sticks and place them in their computers? If so, how often does this happen?

2. Why do people pick up the flash drives?

3. Does this behavior change based on the appearance of the drive, where it is placed, or when it is placed?

We begin by hypothesizing that the attack is effective and primarily exploits either altruism (a desire to return the flash drive to its owner) or self-interest (a desire to profit from the contents of the flash drive). We expect that appropriately configured flash drives can increase compromise rates by playing on these emotions, and that the location and time of day in which the flash drives are dropped will significantly impact the rate of compromise. We hypothesize that these motivations are essentially universal; victims will not differ appreciably in their risk attitudes from the general population.

To test these hypotheses, we designed an experiment in which we dropped 297 flash drives on the campus of a large Midwestern university over the course of two days. The drives were dropped in 30 different locations on campus corresponding to five major types of locations: academic rooms, common rooms, hallways, parking lots, and outdoor areas. The flash drives had varying appearances to appeal to both altruism (drives with keys and contact information return labels attached) and self-interest in the form of curiosity (drives marked "Confidential" and "Final Exam Solutions"). The drives contained plausible folder structures and HTML files that notified our servers (via an img tag) whenever the file was opened in an internet-connected web browser. We collected data which includes information about the flash drives, file open times, and opened files; this data provides insight into which flash drive configurations are most effective. To explore the risk attitudes and thought processes of people who picked up the flash drives, we asked participants who clicked on these HTML files to complete an optional survey. This survey included demographic questions, questions about the flash drives, as well as the Security Behavior Intentions Scale [8] and Domain-Specific Risk-Taking Scale [9]. Seventy-one participants completed this survey.

We find that this attack is effective, even in the presence of alerts shared on social media. While the configuration of the flash drive does not appear to impact compromise rates, the location in which the drive is placed strongly impacts compromise rate. Our file open data, combined with responses to the survey, indicate that most participants are motivated by a desire to return the drive, but we do see that some participants investigate its contents.

We organize the rest of this thesis as follows: in Section 1.2, we describe our research questions and hypotheses. In Chapter 2, we discuss relevant work. In Section 3.1 we describe the research methodology for the USB experiment, and in Section 3.2 we discuss ethical considerations. The results

from the experiment are presented in Section 3.3, while the methodology of and responses to our self-report survey are presented in Section 4.1 and Section 4.2. We discuss the public's reaction to the experiment in Section 4.3. We discuss the implications of our findings in Section 5.1 and contextualize our work by describing methodological limitations in Section 5.2 and avenues for future work in Section 5.3. Finally, we conclude this thesis in Section 5.4.

1.2 Research Questions

We choose to view participants in this experiment through the lens of rational choice theory. This theory states that individuals make decisions by "balancing the costs and benefits of [their] options" [10]. This theory has been applied in other information security contexts as well [10].

We choose to view participants in this experiment through the lens of rational choice theory.

In the case of picking up a foreign flash drive and plugging it into a computer, we hypothesize that most people consider the activity low-risk and are thus more likely to do it.

Therefore, we seek answers to the following research questions:

1. Is this attack viable in the real world? In other words, do people actually pick up the USB sticks and place them in their computers? If so, how often does this happen?

2. Why do people pick up the flash drives?

3. Does this behavior change based on the appearance of the drive, where it is placed, or when it is placed?

We posit the following hypotheses about this data:

- Hypothesis 1: Participants will place the flash drives in computers and click on the relevant files.

- Hypothesis 2a: Participants who pick up flash drives will primarily report doing so for two reasons: to return the flash drive to its owner (an altruistic reason) and out of curiosity/to benefit from the contents of the drive (a self-interested reason).

- Hypothesis 2b: Psychological scales that measure risk attitude will correlate with cybercrime victimization in the general population because participants who believe that picking up the flash drive is too risky will not do so and will thus not be victimized.

- Hypothesis 2c: Participants who picked up the flash drives will have greater risk attitude scores than the general population.

- Hypothesis 3a: The time of day at which drives are placed will not significantly impact success rates because people will quickly pick up the drives once they are dropped.

- Hypothesis 3b: The type of location at which drives are dropped will significantly impact success rates because different location types will attract different demographics and will have different drive visibilities.

- Hypothesis 3c: Altruistically configured drives will have a greater success rate than drives designed to motivate self-interest because participants will be more motivated to plug in the drive if they believe they can help someone by doing so.

- Hypothesis 3d: Both altruistically configured and self-interest-configured drives will have greater success rates than the control group.

1.3 Contributions

In this section, we describe how this study expands on existing work.

We provide a larger-scale experiment than existing studies [11, 12, 13, 14], allowing us to provide more data points about the attack. Each of the referenced studies used 60 or fewer drives, preventing the authors from being able to test different experimental parameters without significantly reducing the experiment's statistical power. Our study involves 297 USB flash drives, nearly five times the quantity used in any of these studies. As such, our experiment, which varies the appearance of the flash drive, the time of day it is dropped, and the location at which is dropped, benefits from the additional drives in the data set. We find that 135/297 (45.45%) of our flash drives were opened after being dropped. Flash drive

appearance and drop time of day did not appear to significantly influence open rates, provided that the drive did not contain any contact information on an external return label. Location appeared to influence open rates.

We provide additional insight into users' behaviors about these drives by providing the results of a survey that includes the DOSPERT and SeBIS scales as well as open response questions. Participants who picked up a flash drive, inserted it into a computer, and clicked on a file were offered the opportunity to complete a survey. In this survey, they were asked questions about their attitudes towards risk taking (the DOSPERT scale) and computer security behavior (the SeBIS scale), along with questions about why they picked up the flash drive and demographic questions. We find that many participants express that they wished to return the flash drive to its original owner. In addition, participants expressed less willingness to try risky activities in all domains except recreational risk and seemed to guard their computers more closely, trust links more, and use weaker passwords. Participants were generally similar to a university population. Their web browser usage was representative of the internet at large, although they used disproportionately more Macs.

CHAPTER 2

LITERATURE REVIEW

2.1 Taxonomy

To highlight the structure of related work in this paper, we present the following explicit taxonomy:

1. Social Engineering
    (a) Similar USB Flash Drive Studies
        i. Peer-Reviewed Studies
        ii. Anecdotal Evidence
2. Human Decision-Making
    (a) Risk Attitude Scales
        i. Developed Scales
    (b) Correlates of Cybercrime Victimization
        i. Only Surveys
        ii. Other Risk Factors
    (c) Perceived Risk
        i. Correlated Factors
        ii. Evidence of Attitudes
    (d) Online Behaviors
        i. Correlated Factors

We discuss recent social engineering work to illustrate recent developments in the field; similar USB flash drive studies show the current knowledge on

this topic and provide useful guidance for the design of our study. This review corresponds to our first and third research questions.

As one of the major contributions of this paper is insight into the thought process of participants in the experiment, we heavily refer to work in human decision making. We present scales that have been developed to measure perceived risk in other contexts, including the two scales that we use in this work. We also highlight work that indicates the default risk perception state of various populations. Finally, we present a selection of studies that attempt to determine correlates of actions related to risk. Broadly speaking, these studies fall into three categories: risk attitudes, online behaviors, and cybercrime victimization. Risk attitude correlate studies attempt to correlate factors with the perception that an act is risky, while online behavior studies attempt to correlate factors with the likelihood that a participant would either perform a beneficial security behavior (e.g., use a strong password) or a harmful one (e.g., click on a link in an e-mail from an unknown sender). Cybercrime victimization studies attempt to correlate factors with the knowledge that a participant has fallen victim to some form of cybercrime in the past. Prior work of this form influenced the survey instruments used in this study.

2.2 Social Engineering

In this section, we discuss recent work in social engineering and previous applications of USB-based attacks in order to highlight current knowledge about our first and third research questions.

Modern work in social engineering often emphasizes the low cost of feasible attacks; phishing attacks can be made more effective using social data [15] and automation [16]. It is now possible to attack Bluetooth devices at low cost and without arousing suspicion, even in secure areas [17]. Participants will attempt to access cell phones they find on the ground [18]. Users can even be financially incentivized to run unknown executables at low cost [19]. Some recent work has also been designed to taxonomize and defeat these types of attacks [20]. Our work represents another type of social engineering attack that can be performed at low cost.

Jagatic et al. [15] describe the process of "social phishing," or using pub-

licly available social networking data to improve the effectiveness of a phishing attack. They phished a group of Indiana University students in April 2005; 16% of the control group fell for the generic phishing attack, while 72% of the social group fell for the social phishing attack. In both attacks, recipients were sent a spoofed email with a link to an external site that asked for their university login credentials from a sender with an indiana.edu email address; in the social case, the email was sent from one of the target's connections.

The attack was effective during a short time frame; "70% of successful authentications" occurred within the first 12 hours of the attack. "Some users visited the site (and disclosed their passwords) over 80 times." Women appeared to be more vulnerable to the attack, and "the attack was more successful if the spoofed message appeared to be sent by a person of the opposite gender." Class standing did not significantly impact compromise rate, although major did in the case of the social attack.

The authors also attempted to perform another attack in which the phishing email seemed to originate from a group conversation of friends. However, a coding error caused the email to be sent to the author of the email; this attack still had a 53% success rate.

In forums that were designed to let participants discuss the experiment, subjects expressed anger, denial, and misunderstanding about email and social networking technologies.

Huber et al. [16] explore the possibility of automating a social engineering attack on an organization using a social networking site; automating the attack would reduce cost.

They propose a model for a bot that has 5 different phases: plan, map & bond, execute, recruit & cloak, and evolve/regress. In the planning phase, the attacker provides the bot with "initial parameters" that specify the attack. The bot then connects to appropriate people and chats with them using chat logic that was defined in the chat stage ("map & bond"). Eventually, the bot carries out the attack ("execute") and either deletes the attack account or "tries to recruit the attacked user and her/his circle of friends for future attacks" ("recruit & cloak"). Finally, the bot adapts its behavior based on the effectiveness of the attack (evolve/regress).

The authors mined data from "the five succeeding Sweden-based multinational corporations that are big enough to presumably have a large number of

employees registered on Facebook." This process took 4 hours from start to finish and found 8.4 viable attack targets (single males who belonged to the organization's closed network and who were accessible) on average. "Except from the CAPTCHA that needed to be solved manually in order to create an account for the ASE bot, no technical measures of Facebook banned or blocked the ASE bot."

The authors also recruited 20 university students to perform a Turing test to see if their chat bot was effective enough to be considered a person. The bot was based on annotated Alice AIML (AAA) files. The subjects believed the chatbot was a bot with probability 85.1%, while other subjects believed the control human was human, with a 3.27% chance of being an AI.

Carettoni et al. [17] discuss their experiences with a prototype "covert attack and scanning device" for Bluetooth called the BlueBag. This bag, containing a MiniITX PC running Gentoo and related peripherals, costs approximately $750 to build. The purpose of the bag was to investigate how inconspicuous attack devices could be built for Bluetooth.

In approximately 23 hours over 7 high-traffic areas in Milan, the authors found 1405 discoverable devices. Of these devices, 1312 were smart phones; of these, 313 devices could be scanned for the presence of the OBEX Push service. The authors blame the discrepancy in these two numbers on range; they suspect that most devices have this service active. The authors suggested that the average "visibility time" for these devices ranged from 10.1 to 23.1 seconds in different locations.

The authors also attempted to send a file to all devices with active OBEX Push support; "an astounding 7.5 percent of device owners carelessly accepted unknown file transfers from unknown sources and were thus highly vulnerable to social engineering attacks."

The authors also built a sample Java Bluetooth worm and developed a simulation that would estimate the propagation of the worm using parameters derived from their real world experiences. They found that a single infected device could infect an entire food court filled with a "population of 184 discoverable devices (7.5 percent of which were susceptible to infection)" within approximately half an hour; use of the BlueBag would reduce this time nearly threefold.

During all of these experiments, "at no time did anyone stop us or suspect us of doing something unusual, even in highly secured areas such as airports."

In a study for Symantec [18], Wright left 50 smartphones in 5 different city locations (New York City, Washington D.C., Los Angeles, the San Francisco Bay Area, and Ottawa, Canada). Smartphones were left completely unsecured in high-traffic, publicly accessible locations.

The smartphones contained 12 dummy apps, 4 of which were designed to represent personal applications, 4 of which were designed to represent business applications and data, and 4 of which were designed to be neutral. Two of the business icons were "HR Cases" and "HR Salaries," which were given icons that indicated a PDF and an Excel spreadsheet, respectively. The instrument was designed so that the researcher could record which apps were opened. The "Contacts" app contained an entry with the tag "Me" on it; this included a phone number and email address so that finders could contact the owner of the smartphone directly. These attempts were also recorded.

The smartphones were left in the cities with full batteries within a period of a few days. Data was collected for 7 days.

The author found that 96% (48/50) of the smartphones were accessed by the finders of the devices; 70% of the smartphones had both business and personal applications accessed. Only 50% of the finders contacted the owner to attempt to return the smartphone.

Christin et al. [19] tested to see whether they could financially incentivize users to run an unknown, untrusted binary. In their study, they created an Amazon Mechanical Turk task where users were asked to run a "Distributed Computing Client" from the "CMU Distributed Computing Project." The users were presented with a click-through consent form; however, downloads and data collection were run from a third-party domain and no official CMU websites acknowledged the existence of the project; this was done to mimic what an attacker might try to do to disguise malware as a legitimate university research study.

The program that participants ran collected some data about the user's system and displayed a timer that counted down for a period of time. Half of the time, participants received a version of the binary that requested administrator access, a process that required the confirmation of a User Account Control (UAC) prompt in Windows Vista and Windows 7.

The authors offered five versions of the study, differing only in compensation ($0.01, $0.05, $0.10, $0.50, and $1.00). Participants were only compensated for their work once, and each version of the study was made available

during a different week.

The authors found that a significantly larger fraction of users downloaded and ran the executable when they were offered compensation of $0.50 or $1.00. The authors did not find statistically significant differences in execution between the version of the program that required administrator access (and thus the UAC dialog in some versions of windows) versus the version that did not. Turkers who were paid more were also more likely to have up-to-date operating systems.

The authors also performed a follow-up study in which participants self-reported data. They found that the fraction of people who were expected to have security expertise remained constant across all price brackets. In addition, participants were asked to measure their perception of the risk of running programs from Mechanical Turk using a 5-point Likert scale; on average, participants who were compensated $0.50 or $1.00 perceived the activity as riskier than those were paid less.

Greitzer et al. [20] discuss the unintentional insider threat (UIT) problem and analyze a few related case studies. They define an unintentional insider threat:

> "An unintentional insider threat is (1) a current or former employee, contractor, or business partner (2) who has or had authorized access to an organization's network, system, or data and who, (3) through action or inaction without malicious intent, (4) unwittingly causes harm or substantially increases the probability of future serious harm to the confidentiality, integrity, or availability of the organization's resources or assets, including information, information systems, or financial systems."

They also define social engineering in this context:

> "Social engineering, in the context of information security, is manipulation of people to get them to unwittingly perform actions that cause harm (or increase the probability of causing future harm) to the confidentiality, integrity, or availability of the organization's resources or assets, including information, information systems, or financial systems."

The authors create a social engineering taxonomy based on interpersonal interaction (or lack thereof) and means to accomplish goals (electronic or non-electronic). The authors focus on attacks with interpersonal interaction and electronic means because they are relevant to the UIT problem.

The authors also summarize demographic, organizational, and human factors that were previously discussed in the literature. "We created an incident template to represent UIT social engineering incidents that we have collected from sources such as Internet searches and reports referenced in the literature. Examples are described below (the full set of cases is reported in [32])." They are unable to conclude anything regarding demographics, but identify potentially dangerous organizational and human factors. They create a "kill chain" model for single- and multiple-stage phishing exploits as well as system dynamics models of "Social Engineering of Insiders by Outsiders" and "Avenues for Social Engineering Mitigation."

The authors also provide mitigation and strategy recommendations.

2.2.1 Similar USB Flash Drive Studies

In this portion of the thesis, we discuss other experiments that involved dropping USB flash drives as a means of attack. These attacks helped to inform the design of our own experiment and provide information about how effective these attacks are in general. We compare the results found in these studies with our own in Section 3.3.9. We also describe a related experiment that attempted to determine predictors of whether a participant would attempt to return a dropped USB flash drive; this study also informed our experimental setup. As a large portion of evidence for the effectiveness of this attack is anecdotal, we present anecdotal evidence as well.

Anecdotal Evidence

One of the most-cited anecdotes about this topic is an article written by Steve Stasiukonis [11]. In this article, Stasiukonis discusses penetration testing a credit union. The author used promotional flash drives in the study; the appearance of the flash drives is not discussed further. The author seeded the drives in the parking lot, employee smoking areas, and "other areas employees

frequented" early in the morning. Out of the 20 drives, 15 were ultimately activated by an employee.

One proposal of this type of experiment [21] proposes a study with a sample size of 100 drives and notes that no comprehensive studies have been completed about this effect. It also refers to this process as "USB baiting." The authors look to answer the following research questions:

- What is the tendency and reasoning for users to plugin a foreign USB drive?
  - Do different drop-off environments influence the infection rate?
- Which possible USB attack strategies are the most effective for successful malicious code execution?

The drives used in the study would be loaded with content similar to that of an administrative worker. The authors plan to actually exploit various Windows vulnerabilities, although the flash drive's malware will not actually do anything malicious. As in other studies [14], the authors suggest using HTTP as a callback mechanism to record activation events. They also suggest notifying users that their machines are vulnerable and requesting their feedback to determine why they activated the drives in the first place.

In another experiment, Wright [12] dropped 54 USB drives on the ground and indicated the number of opens. He reported 32/54 (60%) of the drives were opened and 3/54 (5%) of the drives were picked up by a subject who contacted the owner without clicking on a file. There does not appear to be more information about this experiment online.

Another study of interest can be found in a presentation given by Miles McQueen [13]. In this study, the author distributed 50 flash drives (called "road apples" in the presentation) in various outdoor locations at Idaho National Lab. Each flash drive contained an autorun file and an executable disguised as a Microsoft Excel spreadsheet of a salary survey. In the study, 34 of the 50 drives were returned by employees, while 10 were plugged into a computer. In a follow-up study performed 14 months after the initial study (and after employees were educated about social engineering), only 1 out of the 50 dropped flash drives were activated.

Peer-Reviewed Studies

In this section, we discuss studies that have been formalized to a greater degree.

One of the most comprehensive studies of a USB flash drive attack can be found in Jeffrey Jacobs' master's thesis [14]. In this study, Jacobs attempted to answer two different research questions:

1. "Do USB flash drives remain an effective social-engineering vector for cyber attacks targeting commercial computer systems?"

2. "Are USB flash drives an effective social-engineering vector for cyber attacks targeting residential computer systems?"

His experiment was modeled after Stasiukonis [11]. In this experiment, 60 identical Memorex flash drives were dropped on public sidewalks and parking areas in different areas of Maui, Hawaii. Of these drives, 30 were dropped in residential locations, while the other 30 drives were dropped in commercial locations; these two zones were differentiated geographically using data from the Maui County Planning Commission. Jacobs chose to place 30 drives in each area because it allowed him to verify with 95% confidence that the drives had a 10% effectiveness rate.

The drives themselves were 128MB Memorex flash drives; they were colored blue, gray, and white, although the distribution of these colors is not provided in the thesis [14]. Attached to the drives was a printed label that carried a unique first name and last initial pair. These names were selected from an official list of common baby names for the year 1990; half of the names were female and the other half were male. Gender neutral names were not used to label devices.

Each drive contained 5 different HTML files with the names gallery.html, resume.html, budget.html, bookmarks.html, and slideshow.html; their content was designed to resemble a student's assignment. Each file also used an image tag to reference a link containing a unique identifier and security code; when this link was accessed (by loading the html file in a web browser), Jacobs recorded the flash drive's identifier, the file accessed, and the date and time of access. Users were not identified, notified that they participated in a study, or asked to provide any input. Instead, the experiment was designed

to avoid distressing users by designing the files and links so that they did not appear malicious.

The drives were distributed over three different days (Tuesday, Wednesday, and Thursday) in January 2011; 10 drives were dropped in residential areas and 10 were dropped in commercial areas on each day. Drives were placed in different towns on different days and were recollected if they were not picked up after 8 hours. Davis recorded activation for a device if one of its corresponding URLs was accessed within 72 hours of the device being dropped.

Davis found that 11 out of the 30 drives in each of the residential and commercial populations were activated during the time frame that measurement took place. The mean and median times between device drop and device activation were 7.30 hours and 2.69 hours for the commercial population and 14.10 hours and 4.33 hours for the residential population. All but two of those devices were activated within 28 hours; of the two remaining devices, one was activated between 48 and 52 hours after the drop and the other was activated between 56 and 60 hours after the drop. The author was unable to make statistically significant conclusions about the impact on effectiveness of the gender of the name displayed on the flash drive. Davis also attempted to measure the impact of time of day and date on effectiveness but ultimately noted that his experiment was not well-controlled enough to draw significant conclusions.

Finally, we note a study that does not directly mirror the attacks we describe; however, it involves inconspicuously dropping flash drives, which has a direct application to our experimental apparatus. It is meant as a modern test of the lost-letter experiment [22], which was a study to determine popular sentiment toward various groups at the time. In the lost-letter experiment, Milgram, Mann, and Harter dropped letters addressed to various groups in city locations. Each letter contained postage, so participants simply had to put the letter in a mail box for it to be returned to the researcher. In this experiment, the authors found that letters addressed to "Friends of the Nazi Party" and "Friends of the Communist Party" were returned less often than letters addressed to a person or "Medical Research Associates."

Lastdrager et al. [23] modified the lost-letter technique to deal with USB drives. The authors labeled some drives using both male or female names and thesis or music labels and left a control group of drives in their original

packaging. They dropped drives in buildings that had service desks or receptionists; one student dropped drives while others observed people who picked up the drives and if participants returned the drives to the service desk.

They recorded the time of drop-off, time before the drive was picked up, the sex of the dropper, the sex and age of the participant, as well as the participant's number of companions, behavior, and whether the participant was walking towards or away from the service desk. The authors found that new (unopened) drives were returned less often and that drives were picked up quickly.

The main predictors of theft turned out to be the subject's apparent age and whether the subject put the key in a personal container after picking it up.

2.3 Human Decision-Making

This section contains literature discussing various studies detailing the human decision-making process. This information was valuable and informed the design of the survey instrument used in this study.

2.3.1 Risk Attitude Scales

Much academic work has been dedicated to surveying people's perception of risk. In one such study [24], Weber, Blais, and Betz describe a domain-specific scale that measures risk attitudes in five different domains. These domains were selected based on a meta-analysis of the literature and other existing scales. The authors do not describe the process of choosing initial item candidates in significant detail.

The items in this scale were refined over three different surveys. In the first survey, Weber et al. presented a set of 101 different items that spanned the 5 categories. Each item was presented twice: once for the Risk-Behavior scale ("... indicate your likelihood of engaging in each activity") and once for the Risk-Perception scale ("... indicate your gut level assessment of how risky each situation is"). The authors then reduced the scale to 50 items by picking the 10 items from each subscale with the highest item-total correlations for that subscale. The second survey was designed to establish test-retest

reliability and validity. The third survey consisted of 64 items: the refined 50-item scale from Survey 1 (with some reworded items) and 14 additional items designed to "improve item quality." The scale was then reduced to 40 items by picking the 8 items from each subscale with the highest item-total correlations.

In all surveys, items were interspersed with items from other subscales. The order of the items was also randomized.

The authors also attempted to fit a 6-factor model to their results.

Weber et al. found strong support for the domain-specific nature of risk. In addition, their results suggest that risk-taking is primarily driven by individuals' perception of a particular risk, rather than their attitude towards that risk.

In a future study [9], Blais and Weber reworded and refined their 40-question scale so that it is now 30 questions long. We use this shortened scale to measure domain-specific risk perception in this work.

Egelman and Peer [8] developed a scale that measures participants' willingness to follow good security advice. Using an iterative process, the authors refined a list of 30 items found during literature review and discussion with experts into a 16-item scale split into four subscales corresponding to device securement, password generation, proactive awareness, and updating.

Participants in studies to refine the scale were taken from Amazon's Mechanical Turk platform and were roughly representative of the U.S. online population. The authors removed questions from the scale that were non-applicable, had poor item-total correlations, or exhibited ceiling effects. Participants did not appear to demonstrate any social desirability bias. After sufficient refinement, the authors applied exploratory factor analysis to an intermediate 24-item version of the scale and found four factors. Further refinement removed 8 items from the scale and produced a scale with 16 items loaded across the four factors (each of which ultimately represented a subscale). Overall, 3,619 participants were included in this process.

Egelman and Peer establish that this scale is reliable, displays discriminant validity with regards to the Privacy Concern Scale [25], loads on the same factors in multiple administrations, and displays test-retest reliability. After correlation with other psychometric measures, the authors find that portions of the DOSPERT correlated (albeit weakly) with their scale and that the Consideration for Future Consequences scale [26] appeared to correlate best

with their scale.

We include this scale in our survey because we wish to determine the self-assessed security behaviors of participants who picked up the flash drives.

Some studies have alternately attempted to determine factors that explain why an activity is perceived as risky. Fischhoff et al. [27] discuss an approach to determine whether something is "safe enough." This approach, called "expressed preferences," "employs questionnaires to measure the public's attitudes towards the risks and benefits from various activities." This is in contrast to the "revealed preference" approach, which uses historical data. "The goal of the present study is to evaluate the usefulness of questionnaire techniques for investigating issues pertaining to risk-benefit tradeoffs."

The authors used 76 members of the League of Women voters as participants in their study. Each participant was asked to rank and rate perceived risks or perceived benefits of 30 different activities, as well as provide information on "the acceptability of its current level of risk," and "its position on each of nine dimensions of risk." For the ranking and rating task, participants were asked to rank the activities and assign ratings based on how they compared to the least beneficial (or risky) item. These least beneficial items were assigned a score of 10, and other items were to be scored proportionally (i.e., "a rating of 12 indicates that the item is 1.2 times as beneficial as the least beneficial item").

For the "acceptability of risk" scale, participants were asked to judge whether activities needed "serious action, such as legislation" to make them safer, whether they could be more risky, or whether the current level of risk was acceptable. In the first two cases, participants were asked to provide multipliers.

Finally, participants were asked to provide ratings on 7-point Likert scales for each of 9 factors that were "hypothesized to influence perceptions of actual or acceptable risk."

The authors found that "perceived risk declined slightly with overall benefit," which is a different result than other studies. "Perceived risk was correlated 0.75 and 0.66 with risk adjustment factor ratings for the risk and benefit groups, respectively." The authors also inferred that "participants in our study believed that more risk should be tolerated with more beneficial activities." The authors also found that many of the 9 factors were intercorrelated, so they could be reduced to two factors. "One dimension ap-

parently discriminated between high- and low-technology activities, with the high end being characterized by new, involuntary, poorly known activities, often with delayed consequences. The second dimension primarily reflected the certainty of death given that adversity occurs."

2.3.2 Correlates of Cybercrime Victimization

This section describes studies that examined the relationship between cybercrime victimization and either a survey or a combination of factors (which may include a survey). This helped us to develop our survey instrument by providing material for questions that could be correlated with picking up and using the flash drives.

Only Surveys

Welsh and Lavoie [28] attempt to apply the Routine Activities Theory (RAT) to the domain of cyberstalking. In this theory, described in [29], victimization risk is modified by three significant factors: motivated offenders, suitable targets, and effective guardianship (which represents attempts to prevent the crime from occurring).

The authors analyzed survey responses from 321 female undergraduate students. They measured the relative exposure of the respondents as targets by creating a 17-item survey that asked respondents to indicate how frequently (on a 5-point Likert scale) they used the internet for different activities. They also created a self-report Online Disclosure scale; for each of 24 different pieces of personal information, participants were asked to rate (on a 5-point Likert scale) how likely they would be to reveal this information on a social networking site. The authors used the 30-item DOSPERT scale [9] to evaluate the participants' risk attitudes. The Cyber-Obsessional Pursuit (COP) scale [30, 31] was used to measure the participants' extent of cyber-stalking victimization experiences.

The authors found that Social risk taking in the DOSPERT was correlated with cyberstalking victimization outcomes, as well as more time spent on social networks and additional information disclosure.

Bossler and Holt [32] also attempt to apply RAT to explain cybercrime. In this study, the authors analyzed 570 responses from a self-report survey

of undergraduate students.

The authors measured victimization that caused respondents to lose computerized data due to malware infection. Originally, the authors attempted to measure how many times someone was victimized in the past 12 months, but less than 7% of the sample was victimized more than twice; the authors thus decided to treat the dependent variable as a dichotomy (no malware-related loss versus malware-related loss) and attempt to determine which activities and patterns are related to this loss.

In addition to various demographic questions (including internet connection speed), the authors asked respondents to describe how much time they spent per week (on average) on six different types of activities online. Respondents were also asked whether they avoided using online banking systems or social networking websites.

Deviant computer behavior was measured by asking respondents how many times in the past 12 months they committed software piracy, committed media piracy, watched pornographic or obscene materials, attempted to guess someone else's password, accessed someone's computer without their knowledge, modified or printed computer information without the owner's knowledge, and accessed another's wireless internet connection without their permission. The password, computer access, and modification questions were averaged to create a "hacking score"; this score was averaged with the remaining four items to create a deviancy score.

Respondents were also asked questions that dealt with personal, physical, and social guardianship. Personal guardianship was assessed by asking a single question about the respondent's computing skill level. Physical guardianship was measured by asking respondents whether they had various types of security software (or hardware firewalls) and whether they visited Microsoft Update. Social guardianship was measured by asking respondents to choose an item on a four-point scale that represented the fraction of their friends that performed one of the items mentioned in the deviant computer behavior scale (software piracy, media piracy, pornography, or hacking) in the past 12 months. As before, the hacking scale was made up of three averaged items.

The authors found that pirating media correlated with computer infection, as well as having friends who viewed pornography. Personal and physical guardianship are relatively insignificant in predicting infections that lead to data loss.

Ngo and Paternoster also attempt to link individual and situational level factors to cybercrime victimization [33]. They operate from the Routine Activity Theory and General Theory of Crime perspectives and attempt to determine whether their components correlate with different types of cybercrime victimization. The seven chosen types of cybercrime victimization are "computer virus, unwanted exposure to pornographic materials, sex solicitation, online harassment by a stranger, online harassment by a non-stranger, phishing and online defamation."

Data for this study was collected via voluntary participation on a university campus. A total of 295 students completed a survey; due to the university's commitment to a non-traditional degree program, participants were not representative of "a typical U.S. university." As the dependent variable, "respondents were asked if they experienced each of the ... forms of cybercrime victimization in the past 12 months." Respondents were asked to complete a scale designed to measure self-control. Questions about participants' frequency of online activities (exposure to motivated offenders), participation in potentially risky behaviors (target suitability), and experience in working with computers and computer security configurations (capable guardianship) were used to test the routine activities theory. As control data, the authors also collected demographic info (sex, race, employment, and marital status) and measured "computer deviance" by asking whether participants had performed each of five different actions in the past 12 months.

The authors applied logistic regressions to their results. By regressing on low self-control and holding control data constant, they found that low self-control significantly correlated with both forms of harassment. Race, age, and employment appeared to significantly predict some forms of victimization in this regression. By regressing on the RAT measures and control data, they found that time spent instant-messaging correlated to harassment by non-strangers. Surprisingly, clicking and opening unknown links was negatively correlated with virus infection, the measure of installed security software was positively correlated with virus infection and harassment by a stranger, and the measure of computer crime education was positively correlated with unwanted pornography. The authors argue that the RAT results are weak, especially considering the presence of multiple comparisons.

Both age and employment were found to negatively correlate with harassment by a stranger. The computer deviance scale was positively correlated

with harassment by a non-stranger, unwanted pornography, and phishing.

Other Risk Factors

Lévesque et al. [34] provided 50 test subjects with laptops and monitored their activities over the following four months. The laptops were configured identically at the beginning of the study and contained a Trend Micro antivirus product as well as other process exploration and anti-malware tools and Perl scripts used to collect data about the experiment. The researchers collected information about installed programs and browser plug-ins (and available updates for programs), web browsing, internet connections, and time usage.

The authors found that 38% of the users were exposed to malware that was detected by the antivirus over the course of the study. The vast majority (over 85%) of the detected malware was made up of Trojans. In addition, 20% of the users installed threats that were not detected by the antivirus. The authors found that gender, age, employment status, and work/study domain did not have any statistically significant impact on infection rate. However, the authors did find that users with a high level of computer expertise (defined as users who "configured a home network, created a web page, and installed or re-installed an operating system on a computer") were significantly more likely to be infected at least once than low-expertise users, although they were not significantly more likely to see a larger number of infections than low-expertise users.

Behaviorally, users who visited more websites and installed more applications were at a greater risk of being infected. The authors also found that visits to media-sharing and pornographic sites were correlated with malware infection, although sites that contained content relating to internet infrastructure and sports were more highly correlated with infection.

Levesque et al. also use this data [34] to develop a model that will predict users' risk of malware victimization [35]. As before, users whose computers were infected at least once during the course of the study (n = 23) were placed in the high risk group, while users who were not infected were placed in the low risk group (n = 27). The goal of this study was then to predict which risk category a user belonged in.

The authors used computer expertise, age, total number of hours connected

to the internet, total number of web sites visited, number of files downloaded, most used web browser, and the number of visits to {peer-to-peer, software download, streaming media/mp3, email, social networking, pornography} sites.

The authors built a MLP neural network out of this data, using 60% of the data for training, 20% for test, and 20% for validation. Only 45 users' data were used for this part. "We trained up to 20 models and selected the one with the best predictive results." The overall accuracy of this model was 80.85%. The authors do not consider this great prediction performance.

The authors intend to also do this with self-reported data. They are the first to combine real-world usage data with social-demographic factors.

Canali et al. [36] attempt to predict the risk that a user will visit a malicious web page based solely on their browsing data. To accomplish this, the authors analyzed the 3-month user-initiated HTTP browsing data of 160,229 client machines (provided by Symantec), extracted 74 different attributes that summarized this behavior, and then attempted to see if any of these attributes effectively classified users as low-risk or high-risk. In this study, low risk users never encountered malicious websites or blacklisted domains, while high-risk users encountered at least two malicious URLs or three blacklisted domains. Malicious webpages were classified using various lists, and were classified separately from blacklisted domains. This classification was performed in an automated fashion on Symantec's servers; the URLs were anonymized by reducing them to their fully-qualified domain names for human analysis. Analysis was only run on clients who visited at least 100 web pages over the time spanned by the data.

The authors found that users who visited more URLs, domains, and hostnames were more likely to visit malicious websites. In addition, visiting pornographic and adult websites, surfing webpages with a top level domain different than .com, .net, or .org, having a larger amount of web activity, visiting fewer websites in the Alexa Top 500, and visiting web pages with a larger number of languages were weakly correlated with risk.

Maier et al. [37] attempt to study the conventional wisdom that residential users often experience "compromise and infection" on their networks. They also wished to study whether "security hygiene" (doing things like frequently installing OS or antivirus updates) or risky behavior (accessing URLs blacklisted by Google's Safe Browsing API) correlated with signs of

compromise. The authors "search for three behavioral indicators—address scanning, port scanning, and spamming—and also monitor for network-level signatures aimed at detecting three malware families, Zlob, Conficker, and Zeus."

The authors analyze traffic from four different sources: a European DSL provider, a community network in rural India, dorm users in a large US university, and LBNL. The authors found that residential systems displayed a relatively low amount of malicious activity. They also found that accesses to URLs that correspond with AV updates or Windows Update did not impact the likelihood of being infected with malware, while connecting to malicious sites (that their browsers should have warned them about) increases the risk that a computer is infected with malware.

Yen et al. [38] study malware encounters in a large enterprise. They used McAfee anti-virus reports on 85,000 machines, as well as Windows authentication logs, web proxy logs, VPN logs, and the employee database to provide information about properties of malware compromise.

The authors limit their analysis to hosts that are logged onto by one user most (80%) of the time. They observed the enterprise over 4 months and found that of 62,884 primary-user-identified machines, 9,625 generated malware reports.

By looking at the file system location where malware is found, the authors identify that external drives are the most prevalent location of malware encounters. However, both the malware encounter rate and the file system location distribution depend on the country that the hosts are located in. Most malware reports reach the central data collector more than 10 minutes after infection is detected, suggesting that hosts most frequently encounter malware outside of the network. However, this factor also differs by geography.

A user's distance from the CEO in the corporate hierarchy and the technicality of their job title positively correlate with malware encounters. The authors argue that this is the case because lower-ranked users may be more technical.

The authors match 390 McAfee reports with web proxy logs and find that most of the malware in this data set comes from innocuous categories (e.g., "Business") and was allowed through the proxy.

The authors also built a logistic regression model using demographic, VPN

activity, and web activity features. They find that, among other features, a user's rank, the technicality of a user's job title, the total number of domains a user has visited, and the number of HTTP connections to chat, file transfer, social networking, and non-categorized sites a user has visited contribute significantly to the model. When the authors applied their model with all 20 features combined, the top 1000 riskiest hosts (as predicted by the model) had a malware encounter rate of 51% (as compared to 15% for the entire enterprise).

2.3.3 Perceived Risk

This subsection describes studies that examined perceived risk. This information serves to highlight the current state of knowledge of how "normal" populations perceive risk.

Correlated Factors

In [39], Garg and Camp conduct a survey to determine what factors primarily influence risk perception; to accomplish this, they used Fischhoff et al.'s nine-dimensional model [27]. Example dimensions include immediacy (whether the threat happens immediately or later in time), knowledge to the exposed, and severity of consequences.

In the survey, participants were asked to rank fifteen different security and privacy-related phrases in order of perceived risk. Example terms included "identity theft," "cookies," and "virus." Participants were also asked to rate each item they were familiar with for each of the 9 dimensions; ratings were done on a 5-point scale, where the meaning of a particular value varied based on the dimension being studied. 93 participants were surveyed as a convenience sample at Indiana University; the authors argue that the literature suggests that the use of this convenience sample should not significantly limit their results because other studies have found out that gender and age did not correlate with different perceived risk scores.

The authors found that the original nine-dimensional model explained a relatively small percentage of the variance in risk perception. They reduced this model to four dimensions and determined that the temporal impact di-

mension (which consisted of the combination of the "newness" and "common-dread" dimensions) was the most significant.

LeBlanc and Biddle [40] also attempt to adapt Fischhoff's model [27] to the computer realm. They included "five non Internet-related activities, and 15 Internet-related activities" in this scale and measured perceived benefit, perceived risk (where the risk was defined as "loss of personal information" instead of death as in [27]), likelihood, immediacy, delay, severity, and frequency of usage on 7-point Likert scales. Ninety-four participants on Mechanical Turk were asked to respond to the survey.

The authors divided various activities into different categories. Activities that involved "potential for embarrassment" were ranked higher on the likelihood scale than on the severity scale; "financial" risks were generally judged to have greater severity and "other" activities lay in the middle of the line. PCA on the two scales with two factors was inconclusive. Hierarchical clustering using complete agglomeration revealed that activities generally fall into the three categories originally speculated by the researchers. Users also appeared to believe that "activities with a certain amount of risk would be paired with a relatively quick loss of personal information in the event that an attack took place." Users seem to believe that some activities (such as online banking and using search engines) are relatively unlikely to cause information loss.

Evidence of Attitudes

Felt, Egelman, and Serge [41] survey users about their opinions about various risks associated with privileges in smartphones. The authors argue that existing resource permission warnings were "not grounded in user research as far as we are aware, and usability problems have emerged as a result." In this paper, the authors "performed two surveys to rank the level of user concern about a wide range of smartphone resources. In our first survey, we asked 3,115 smartphone users to rate their level of concern about 99 risks corresponding to 54 smartphone permissions." "We also asked users about past negative experiences with applications to measure the frequency of risks. In our second survey, we asked 42 smartphone users to state their reactions to low-ranked, medium-ranked, and high-ranked risks."

In the first study, respondents were asked to provide a response on a 5-

point Likert scale (ranging from "Indifferent" to "Very Upset") of how upset they would be if an app performed a particular activity "without asking you first." Each respondent only saw 12 of the 99 possible questions. They were also asked "to tell us about instances in which they had uninstalled 'misbehaving' applications." In the second survey, respondents were asked to provide information about how they would feel, why, and what they would do for each risk that they were presented. Each respondent saw one of the top three risks from the first survey, one of the middle three, and one of the bottom three. Risks were ranked by the fraction of participants who answered "Very upset" in the first study.

The authors found that users were primarily concerned about risks that caused financial damage or permanent damage to data. In the case of these high-concern risks, users expressed willingness to perform actions such as contacting the authorities or pursuing legal action (19% and 12% on average, respectively); conversely, 21% of respondents were willing to do nothing for the low-ranked risks. The authors also note in particular that location information "is not a high-ranked user concern."

Chin et al. [42] present the results of semi-structured interviews with 60 participants. These interviews were designed to determine how willing users were to handle sensitive information on their smartphones versus their computers and "why and how they select applications, which provides information about how users decide to trust applications."

In these interviews, participants were asked to fill out surveys about the demographics of their smartphone and laptop usage ("how many applications are installed on the device"), asked to "rank the factors he/she used when selecting... applications" using card sorting, asked to record information on installed applications for each device, interviewed about their willingness to perform nine tasks on each device, and asked to compare the magnitude of their privacy and security concerns between their smartphones and laptops and to verbally explain their "primary concerns" in the case of their smartphones.

The authors found that users were less willing to work with online shopping, online banking, health information, and their SSNs on their smartphones. About 10 out of the 60 participants specifically cited security reasons for why they would not perform the activity on their smartphones (except for SSNs, where 36/60 people cited them). "Participants are more concerned

about privacy on their phones." Participants were often worried about phone loss, frequently citing important data that was stored on the phone and "expressed doubt in the trustworthiness of the applications." The authors also found that users were more willing to experiment with applications in the mobile realm. They make various recommendations to improve mobile application stores.

Flinn and Lumsden [43] ran a survey to begin to explore "the extent of users' awareness, knowledge, and range of perspectives concerning" " privacy and security tools available in contemporary Web browsers." The authors also wanted to explore anecdotes in the field. Users were asked personal and computer demographic questions, as well as "the same pattern of five questions for each of the four technologies of interest (secure sites, cookies, privacy policies and trust marks)."

> "The first question in each section asked whether the respondent had any previous knowledge of the technology; only when respondents indicated that they had previously heard of it were they required to complete the rest of the questions in the associated section. The second question in each section asked respondents to describe in a few brief sentences what they understood about the technology. The third probed their beliefs about the technology by listing a number of statements pertaining to the technology and asking them to indicate the degree to which they agreed or disagreed with each statement; the statements and the five-point Likert scale response options for each were collectively presented using a matrix-style format. The fourth question assessed respondents' familiarity with the technology in question, and the fifth explored the degree to which respondents' feelings of security and privacy depend on the technology."

A total of 237 users were surveyed.

The authors found that respondents interpreted the phrase "secure site" in two different ways: whether the site contains a "secure connection," or whether the site's "hosts, servers and databases" were secure; users tended to trust the latter more. Generally, users appeared to have significant misconceptions about how secure sites worked, understood cookies better than other technologies, were "skeptical" of privacy policies (but believed that

their creators followed them), and were less aware of how to effectively verify trust marks.

Friedman et al. [44] conducted a study where "Seventy-two individuals, 24 each from a rural community in Maine, a suburban professional community in New Jersey, and a high-technology community in California, participated in an extensive (2-hour) semi-structured interview about Web security." In part of the survey, participants were asked to identify their "concerns about risks and harms from Web use." Suburban individuals identified risks to people ("concerns related to human experience, social relations, or societal issues") more than the other groups, and high-tech individuals identified information risks ("concerns related to the quality, use, and protection of information") more than the other groups. "Across the three communities (that varied with respect to technological expertise and education), users most often emphasized security, privacy, and threat to computer systems."

Koved et al. [45] discuss new risks in security that are created by new mobile device adoption. The authors completed a study that had users indicate "the security risks they perceive when using mobile devices" in "specific scenarios," "including the use of an app and the web to do personal banking, accessing confidential company information, accessing medical information, and using a credit card with an unknown online retailer."

> "The four primary categories of risk emerging from the study are: shoulder surfing, network attacks, compromise of the device, and untrustworthy remote service providers. All of the identified risk factors relate to the loss of personal or confidential information, including passwords. Larger consequences of loss, including access to personal or company accounts, financial loss, identity theft, and publication of private information, were also identified by the study participants. Another category identified by respondents is risk associated with using a mobile device in a particular situation, e.g. personal safety."

The authors now intend to determine where actual risks and perceived risks are mismatched and "where there is a mismatch, risk communication with the user will be considered as a means to align user and system perceptions of risk." The authors hope that "there is greater likelihood that users will

accept and comply with organizational security requirements such as multi-factor authentication methods," which they argue are necessary in the mobile realm.

2.3.4 Online Behaviors

This subsection describes studies that examined the correlation between factors and online security behaviors. This information also helped to inform the design of the survey instrument.

Correlated Factors

Onarlioglu et al. [46] attempted to measure how internet users reacted when faced with concrete web security scenarios. To do this, they created 44 different scenarios in three different test suites (web-based attacks, email-based attacks, and file sharing-related attacks). While participants were told that the study would take about an hour, participants were allowed to leave the study and resume their progress at any point. Participants were not compensated; the survey was promoted as an opportunity for participants to test their security knowledge and get feedback. A total of 164 participants completed the survey, although the file-sharing suite was only given to participants who had encountered BitTorrent or one-click hosting services before.

In most of the tests, participants were presented with screenshots of various scenarios and were asked to indicate their risk perception of the scenario on a 5-point Likert scale; furthermore, participants were asked whether they would perform the relevant activity (such as clicking a link or downloading a file) and why. In one part of the file sharing tests, participants were directed to interactive torrent download pages reproduced from The Pirate Bay and isoHunt and asked to click on the real download link (as opposed to advertisement banners masquerading as download links). A similar test was applied for the one-click hosting providers.

The authors divided the participants into three different groups for analysis. Non-techies are users who worked in non-technical fields and had little to no programming experience. Techies are users in technical fields who have not focused on computer security. Experts are users who are computer security professionals.

The authors formed a security score by calculating the number of questions a participant correctly avoided as malicious (or correctly followed as benign), normalized (to account for the fact that some participants did not complete the file sharing tests) and scaled from 0-100. They also created a risk perception score by correctly identifying risky situations as risky and benign situations as low-risk. This score was also normalized and scaled from 0-100.

Analysis indicated that while the non-techies and experts differed significantly in both their risk perception and security scores, techies did not differ significantly from either of the other groups. Techies and experts only had higher scores at a statistically significant level on the web-based attacks. They also found that the risk perception score positively correlated with the security score, although this correlation was weaker for non-techies ($\rho = 0.5, p = 9.99 \cdot 10^{-6}$) than the combination of techies and experts ($\rho = 0.70, p = 6.51 \cdot 10^{-15}$). Demographic data also did not appear to affect the security score.

In the trick banner tests, non-techies performed significantly worse than techies and experts. Non-techies also demonstrated that they did not have a solid understanding of URL-shortening services.

Milne et al. [47] looked at the relationship between online risk and online behaviors using a protection motivation theory approach, which states that

> "consumers' motivation to protect themselves depends on the severity of the threat, perceived likelihood of the threat, and self-efficacy. Self-efficacy is defined as one's belief in their ability or capacity to accomplish a task or deal with changes such that their actions will have the desired outcome."

The authors looked at adaptive behaviors, which are "actions taken with a business to keep information safe" and maladaptive behaviors, which are "avoidance responses that are driven more by a general fear of online shopping." They also hypothesize that perceived online privacy threat and perceived likelihood of online privacy threat decrease the likelihood that participants will engage in risky behaviors. They also expect self-efficacy to moderate this relationship by weakening the link between these scales and risky behaviors and enhancing the link between these scales and protective behaviors.

Questions for the survey were drawn from the literature and refined with the help of expert survey researchers and a pretest sample of 45 college students. Participants for the actual survey were recruited from an opt-in consumer survey panel; the authors received 449 complete responses from 4000 requests. The authors used PCA to divide 49 behaviors into risky and protective groups.

The authors found "a positive relationship between perceived online threat and maladaptive behaviors and a positive relationship between likelihood of threat and adaptive behaviors," as well as "a positive relationship between adaptive and maladaptive behaviors." Self-efficacy was also found to correlate with more adaptive behaviors and fewer maladaptive behaviors, and fewer risky behaviors taken. However, the authors also found that perceived online privacy threat or likelihood of online privacy threat did not have a significant impact on risky behavior. However, perceived likelihood of online privacy threat did have a marginally significant ($p < 0.10$) impact on protective behavior. The authors suspected positive response bias towards protective activities versus risky ones.

Vance et al. [48] measure the effectiveness of observing an electrical component in the brain using electroencephalography (EEG) as a predictor for actual risk behavior. The authors argue that this approach is promising because self-reported risk perception data has been found to correlate little with actual risk behavior in other work.

Brains were measured by having participants complete the Iowa Gambling Task, a game where participants select cards from one of four decks. The values on the cards represent either gains or losses of money; the decks are arranged with different expected values. Participants are asked to determine which decks "yield the most money in the long run." Participants' risk attitudes are determined based on which decks they pick.

Participants were asked also asked to complete what they were told was an image categorization task on their personal (or the researchers' personal) computers. Periodically, users were given security warnings that were similar to Google Chrome's when a malicious website is accessed. Users who accepted the warning were penalized in terms of their performance for the task. The authors also received a simulated security incident in the middle of the test where a malware-esque screen appeared.

The authors found that none of the self-reported measures of risk per-

ception accurately predicted security warning disregard but that the EEG measures did successfully predict it before the security incident.

Rhee et al. [49] attempt to apply social cognitive theory, which deals with "how perceptions of self-efficacy affect people's motivation and action" [50] (cited in [49]) to understand factors that influence good user security behaviors; they do so because they believe that other work primarily focused on deterring specific bad user behaviors. The punitive approach does not effectively control users' accidental security mistakes.

The authors hypothesize that general controllability, security breach incidents, and computer/internet experience all influence (domain-specific) self-efficacy in information security, which then influences security technology adoption, behavior, and intention to strengthen security effort.

A total of 415 graduate students in business participated in a self-report study where they were asked items from scales adapted from the literature to measure each of the items in the model. The authors built a structural model based on the results and found that all of the hypothesized relationships existed in a statistically significant form. Computer/internet experience most strongly affected self-efficacy, which in turn primarily influenced security technology adoption.

Benenson et al. [51] tested to see whether Facebook users were more likely to click on suspicious links than users who used emails. In their study, they sent users a short message connected to an individualized link and recorded whether users clicked that link. The authors also "invited all study participants to take a survey with several questions about their handling of messages from strangers, their perception of Facebook's security and the reasons why they clicked or not clicked on the link in our message." In both cases, subgroups were formed based on the gender of the sender and receiver; a "neutral" gender (email address) was possible with email but not with Facebook. In the case of Facebook, three different levels of privacy settings were used with each profile and the researchers sent recipients friend requests half of the time. The experiment used 240 Facebook and 158 email participants and 339 participants participated in the post-survey.

The researchers found that participants were significantly more likely (56% vs 35%) to click on the link if responding via email. Participants were also more likely to respond to the message if it was on Facebook. However, profile appearance, the presence of a friend request, or gender of either the sender

or receiver did not affect click rate. Only 17% of all participants reported clicking on the link in the survey, while 39% of all participants actually clicked the link in practice.

> "65% of all survey respondents (220) said that they do not click on Facebook links in messages from unknown senders. Moreover, 67% (228) of all respondents said that they do not click on links in the emails from unknown senders. In the experimental setting, 62% of all Facebook recipients did not click, and 44% of all email receivers did not click on the link."

CHAPTER 3

USB EXPERIMENT

In this chapter, we present the methodology and results from our USB flash drive experiment. The matter in this chapter is designed to provide an answer to our first and third research questions:

- Is this attack viable in the real world? In other words, do people actually pick up the USB sticks and place them in their computers? If so, how often does this happen?
- Does this behavior change based on the appearance of the drive, where it is placed, or when it is placed?

3.1 Methodology

3.1.1 Technical Setup

In this experiment, we used a methodology similar to the one in Jacobs' thesis [14]. We dropped flash drives with varying appearances and varying contents in varying locations across the University of Illinois campus. Each drive only contained HTML files and folders; each file contained multiple extensions (e.g., "resume.pdf.html") so that operating systems that hide file extensions by default would display names that imply other file types (e.g., "resume.pdf"). Each HTML file contained an img tag that referenced a server that the researchers control; when this file is loaded in a web browser, the URL specified by the img tag is accessed, allowing our central server to record that the file has been opened by the user. The HTML file itself contains a debriefing page that indicates to the user that they have participated in an experiment and allows them to consent or withdraw from the study. Users are also provided a link to a survey that they could participate in to provide

information about why they picked up the drive; users who completed this additional step were compensated $10.

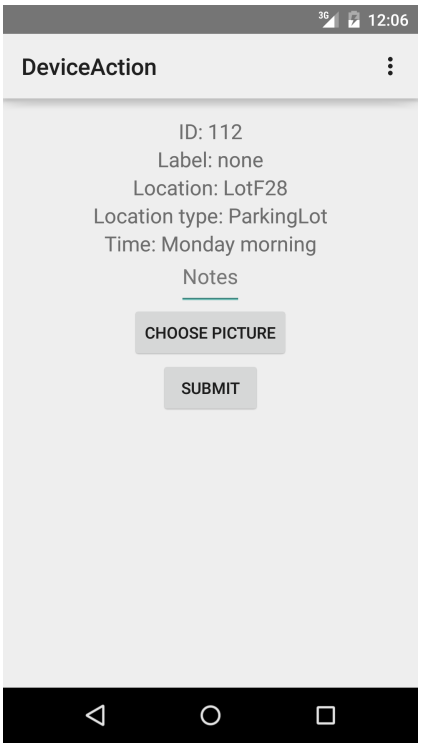
To manage the complexity of a physical experiment of this size, we developed multiple pieces of software to coordinate portions of the experiment. First, we developed software to transform a specification of an experiment (drive configurations, locations, times of day, and researchers) into a schedule where each researcher was assigned some drives (with defined configuration and location) to drop during each drop period. This schedule also divided drives among the different categories used in the experiment. We also wrote another program to send this schedule data to our central server and to use it to program the USB flash drives. In order to more closely track the whereabouts of drives in the field, we developed an Android app that was used while drives were placed. Researchers used the app to store a picture of where the drive was dropped and its GPS coordinates to the central server, allowing them to check to see whether the drives were moved at a later time. Two screenshots of the app, demonstrating the UI for an initial drop and a drive status update, are shown in Figure 3.1.

3.1.2 Distribution of Drives

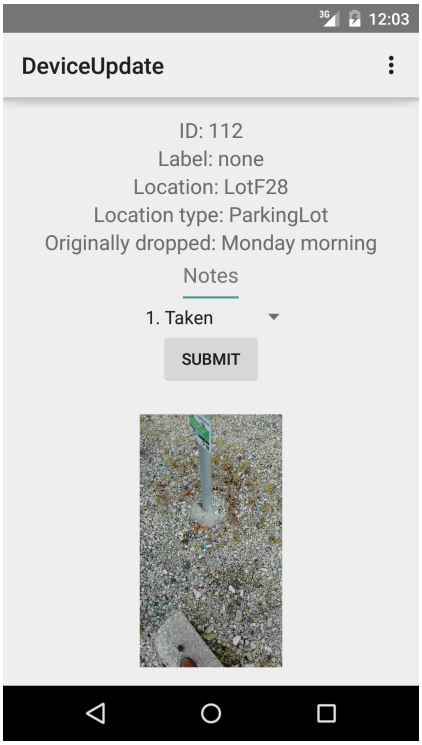
We present this section to describe how we divided the 300 drives among various parameters in the experiment.

We were primarily interested in determining the effects of the time of day that the drive was dropped and the appearance of the drive on pickup rates. As a result, we chose five different appearances of drives and two types of drop times ("morning" and "afternoon"). We wished to test each possible combination of these two variables, so that $\frac{300}{2 \cdot 5} = 30$ drives were dropped for each appearance and drop time.

We also selected 30 locations to drop drives. These locations were chosen based on two factors; first, we divided the University of Illinoiscampus into three parts using east-west streets ("North," "Main," and "South" quads, respectively) and chose 10 locations in each part. We then chose locations that belonged to each of five sub-categories ("Parking Lot," "Hallway," "Outside," "Academic Room," and "Common Room"); each part of campus contained two locations in each category.



(a) A screenshot of the interface to drop a drive. All parameters except the note field and picture are automatically scheduled and provided to the dropper; droppers take their own pictures using their phones and press the "Submit" button to register the GPS coordinates and picture of the drop with our servers.



(b) A screenshot of the interface to update the status of a dropped drive. All fields except the drop status dropdown and note field are provided to the dropper automatically.

Figure 3.1: Screenshots of the Android app used in the experiment.

As we had 30 drives of each appearance and drop time and 30 locations, we simply dropped one drive of each appearance and drop time in each location.

3.1.3 Drive Types

To explore our third research question ("does this behavior change for different drives with different contents"), we chose to drop five different types of drives (see Figure 3.2). One of the drives was left unlabeled, as a control (**None** drives). The remaining four drive types were divided into two groups, with two types related to self-interested behavior and two types related to altruistic behavior.

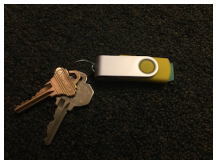
For the self-interest drives, we chose to label drives with labels related to confidential information ("Confidential," **Confidential** drives) and final exam solutions ("Final Exam Solutions," **Exams** drives). We chose final exam solutions in particular because professors tend to distribute previous midterm solutions but closely guard (and re-use questions from) finals; as a result, previous finals are more difficult to find and thus represent a greater opportunity to students and a greater risk to faculty and staff. Confidential information serves to satisfy students' curiosity. These two configurations also represent different self-interest risk-reward tradeoffs. Students caught possessing final exam solutions could face academic integrity charges or expulsion, while students caught possessing other confidential data would likely face fewer significant consequences. However, final exam solutions are more valuable to students than arbitrary confidential data.

In order to test participants' tendency towards altruism, some drives were attached to key chains that contained a few scrap keys (**Keys** drives). Other experiments [52] have argued that participants who attempt to return keys do so for altruistic reasons. In this experiment, we hoped that the absence of identifying information would encourage participants to plug the flash drive into a computer in an attempt to identify the owner and return the keys.

Another group of drives had the same keys attached, although the drives also had a paper label providing contact information for a fake e-mail address controlled by the researchers (**Return Label** drives).

We added this separate group of drives to see whether participants would still plug in the drives even when provided with proper contact information.

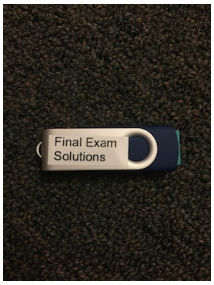
(a) An unlabeled drive.



(b) A drive with keys attached.

(c) A drive with a return label attached.

(d) A confidential drive.



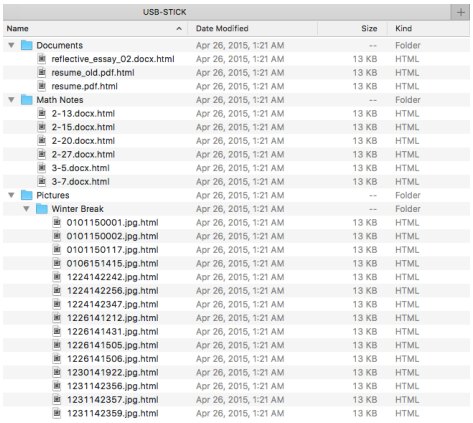
(e) An exams drive.

Figure 3.2: Pictures of the five drive types.

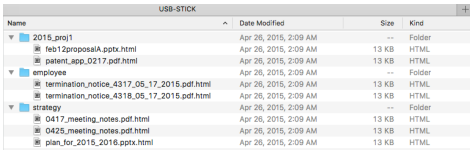
Each drive was loaded with contents that matched its label. These folder structures are shown in more detail in Figure 3.3. All files placed on the drives were HTML documents; each document contained the same content of the debriefing page and the link to the survey. Documents contained a spurious "file extension" at the end of the file name (e.g., "resume.pdf.html"); this was done to mislead careless readers. Some operating systems (primarily Microsoft Windows) will also hide file extensions for known file types; users who have this option enabled will see the filename without the extension ("resume.pdf"), further adding to the deception.

Confidential-labelled drives contained three folders designed to indicate that the resulting drive belonged to an employee ("2015_proj1," "employee," "strategy"). These folders contained file names that implied a proposal and patent application, two termination notices, and two sets of meeting notes and a plan for the future, respectively.

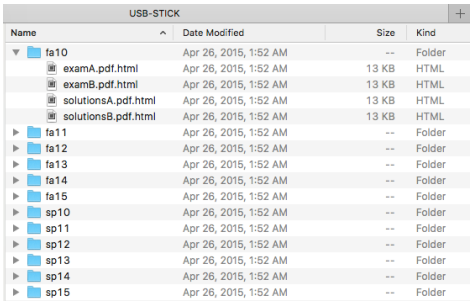
Exam-labelled drives contained a list of folders that represented semesters ("sp10," "fa10," ..., "sp15"). Each folder contained documents labelled "examA.pdf.html," "examB.pdf.html," "solutionsA.pdf.html," and



(a) The contents of unlabeled, keys, and return label drives.



(b) The contents of confidential drives.



(c) The contents of exams drives. Note that only one folder is expanded for brevity; all other folders contain the same file names.

Figure 3.3: Pictures of the folder structures of each of the drive types.

"solutionsB.pdf.html," to represent different versions of an exam. We intentionally omitted any reference to a particular class in order to avoid deterring students who would have little interest in a particular class's exam solutions.

All other drives contained a set of folders and files that were designed to mimic a typical student's personal flash drive. These drives contained three folders: "Documents," "Math Notes," and "Pictures"; each folder contained appropriate content.

3.1.4 Locations

We chose to drop drives in 30 different locations on the University of Illinois campus. The large number of locations was chosen to help avoid arousing suspicion by minimizing the chances that a participant would notice more than one drive while making a particular tip on campus. The campus was divided into three parts ("North," "Main," and "South") based on a campus map [53]; 10 locations were selected from each of these parts.

We also chose to place drives in five different categories of locations; these were divided equally among sub-campuses (i.e., 2 locations per sub-campus belonged to each category). The categories are as follows: **Outdoor** locations represent sidewalks and pedestrian areas in various portions of campus. **Parking Lot** locations represent various parking lots on campus; the University of Illinois requires students to have a permit to access many spaces in these lots from 6am to 5pm (and provides meters for short-term parking otherwise). Parking is otherwise free, exempting 2am-6am Monday-Thursday [54]. Two of the lots used in the study (C9 and F28) allow for overnight parking on the weekends, and all of the lots except one (F28) are primarily intended for faculty and staff use. We chose to choose lots that focused on faculty and staff because we assumed that they would tend to walk between classes less than students would, causing them to be underrepresented in the outdoor sample. **Academic Room** locations represent large lecture halls or library floor space on the University of Illinois campus. We include two libraries in this sample: one on the northern part of the campus that serves primarily engineering students, and the main undergraduate library. We omit the main library because it is located next to the undergraduate library on the University of Illinois campus. **Common Room** locations

represent food courts and publicly accessible locations where students, faculty, and staff may congregate. We include a publicly accessible cafeteria in a research building on the north campus, the lobby of the engineering academic advising building, two lobbies of fitness complexes, the lobby of an undergraduate dorm, and the main food court in the student union in this category. **Hallway** locations include the hallways and corridors of various academic buildings.

We attempted to represent students, faculty, and staff in these locations. Locations that would be visited by students of varying types of majors were included.

3.1.5 USB Survey

In order to collect data about why users picked up the flash drives and to collect data about their risk attitudes, we offered participants who picked up flash drives the opportunity to complete a survey about their risk attitudes for an additional $10 in compensation. We discuss the contents of this survey in more detail in Section 4.1.

3.1.6 Experimental Procedures

This experiment was performed from April 27 to May 1, 2015. These five days span Monday through Friday, and represent a normal week of classes at the University of Illinois. The last day of scheduled classes at Illinois (before finals week) was May 7. On April 27 and 28 (Monday and Tuesday), researchers dropped 150 flash drives on each day. We performed drops during the first two days of the week to reduce the chances that drives would remain on campus during the weekends, when pedestrian traffic patterns change. Drives were dropped in two groups; one group of drives was dropped between the hours of 6am and 10am, and another group of drives was dropped between 1pm and 5pm. We separated these groups by four hours to capture two different behaviors; the morning group was designed to be picked up by faculty and staff going to work, students going to morning classes, and both groups going to lunch. The afternoon group was designed to be picked up by participants who were leaving classes and work. Researchers were not given specific times

to drop specific drives; instead, they were asked to place all of their drives within the specified four-hour period. Researchers were assigned drops that were clustered together geographically to reduce transportation cost and were asked to drop drives in all of their assigned locations on each day to spread out responsibility.

Researchers were instructed to drop drives in plain sight. They were also informed of the protocol that Lastdrager et al. used in [23] to deposit drives: "One student would walk around and pretend to tie his/her shoelaces, look around to see if anybody noticed him/her and drop the USB key before walking away." However, as we wished to record the location of the drives using the mobile phone app, researchers were asked to open their phones and record the location of the drive before walking away. As smartphone use in public spaces is extremely common, we believe that this additional recording step was unlikely to arouse suspicion. Researchers were also asked to occasionally travel in groups with friends to reduce the chances that they would arouse suspicion. One example of a picture submitted to our database can be found in Figure 3.4.

Researchers were also asked to periodically monitor the drives that they dropped. Researchers submitted updates using the smartphone application, indicating that the drive that they were looking for was either **not found, found** (in the same location as dropped), or **moved** (visible, but not in the same location as when dropped). Researchers were instructed not to touch or move the drives and not to interact with any subjects.

In order for us to make meaningful conclusions about the times when drives were picked up, any drive that was dropped during a time period was monitored in the time period immediately following. After this initial monitoring step, drives were monitored daily during the time period in which they were originally dropped. Drives were monitored until they were not found or until May 1, whichever occurred sooner.

3.2 Ethics

As this study required interaction with human subjects, we submitted our project to the University of Illinois's Institutional Review Board (IRB). We obtained IRB approval (represented internally as protocol #15445) before

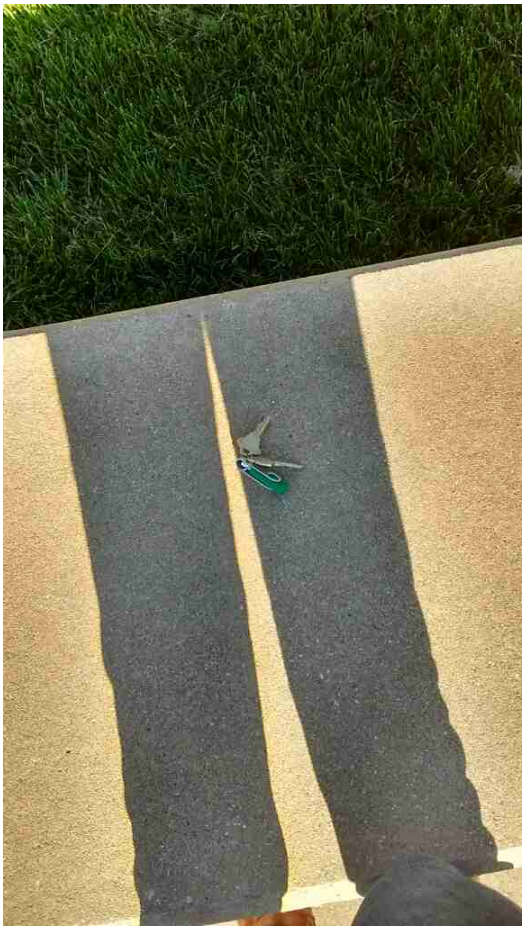


Figure 3.4: A picture of a flash drive placed on a bench outside. This image was uploaded to our database.

fielding the study.

In order for us to determine whether a population is generally susceptible to our attack, we must present it as an attacker would in the real world. As such, we employed deception in this work: we misrepresented the contents of the USB stick using labels and other attachments (such as keys) to give people the impression that they are picking up someone's USB flash drive instead of a research device for a study.

In order to minimize risks to the participants, we attempted to ensure that our USB flash drives will not interact negatively with the participant's system. We did not execute any code on participants' systems; the only files that were stored on the drive were HTML pages that did not contain any scripts.

If a user opened an HTML page stored on the drive, we used the "img" tag to open a URL on a site that we control; this URL was crafted so that it is unique for each HTML file on each USB drive. This information allowed us to track which USB drives have been activated by users. This HTML represented a debriefing form. After reading this form, participants could withdraw themselves from the study or complete a follow-up survey to determine their motivations for picking up the flash drive.

With this in mind, the debrief employed in this study may have caused psychological distress in users who feel that they have been tricked. If the contents of the USB drives are somehow infected, we could have caused damage to the participants' computer systems. In addition, if our website was compromised, we could cause damage to the participants' computer systems by accidentally directing them to a malicious website.

We purchased drives from a reputable vendor. We used Device Manager in Windows to perform a set spot-checks on a sample of the devices and did not notice any unusual values for the vendor and device IDs. We believe that the risk posed by this experiment exists for any person who buys a flash drive from a reputable vendor. As this risk is no more than existing risk, this experiment is minimal risk.

During the experiment, we directed participants to contact us or the IRB if they had any questions, concerns, or complaints. We did not receive any negative feedback from participants; conversely, some participants who returned flash drives to us expressed their appreciation for the research and asked about our results.

3.3 Results

In this section, we discuss the results of our USB flash drive experiment. Data from this experiment was downloaded from the central server on August 31, 2015, for analysis.

3.3.1 Consent and Use in Data Analysis

As our study dealt with human participants, we provided subjects with the opportunity to consent to or withdraw from our data collection. We provided this choice using buttons on the debriefing page when participants opened a file on the flash drive.

We promised participants that "all data about the flash drive" would be deleted if they withdrew from the study or did not consent to have their data collected. As such, we do not include information about the times the drives were opened, what files were opened on the drives, or the user agent strings of each user's browser for participants who did not consent to or who withdrew from the study. However, we do collect aggregate data about the fact that a file on the flash drive was opened, including which categories the opened drive belongs to.

3.3.2 Multiple Comparisons

As the majority of this work involves tests for equal proportions with small numbers of drives, we believe that applying standard corrections for multiple comparisons (such as the Bonferroni correction) would require very large differences of proportions to mark any of the population differences as statistically significant. As one example, 20 comparisons would require $p < 0.0025$ to be statistically significant; in two groups of 60 drives, if one group had 30 successful members, the other would require under 14 or more than 46 successes to be statistically significantly different.

We choose to trade off the risk of a false positive in this study with the risk of marking a real result as not significant by reporting statistical tests in this category using the uncorrected convention ($p < 0.1$, $p < 0.05$, $p < 0.01$). We instead emphasize the exploratory nature of the study and report explicit p values whenever possible.

3.3.3 Number of Opens by Category

In this section, we compare the open rates of various parameters of the experiment to see if any of the experimental parameters appears to influence the rate at which people pick up the flash drives and plug them into their computers.

Flash Drive Label

As discussed previously, we dropped five different types of flash drives with different physical appearances. The open rates for each of these types are shown in Table 3.1 and Table 3.2.

Table 3.1: Opens by flash drive label. Almost all categories of drives were equally effective, with the exception of drives with a return label.

Label	Dropped	Opened	Fraction Opened
Confidential	58	29	0.50
Exams	60	30	0.50
Keys	60	32	0.53
None	60	27	0.45
Return Label	59	17	0.29

Table 3.2: Differences in open fraction by flash drive label. Every other type of drive is significantly more effective than drives with a return label.

	Confidential	Exams	Keys	None	Return Label
Confidential		0	-0.033 (p=0.859)	0.05 (p=0.719)	0.212 (p=0.031)
Exams			-0.033 (p=0.855)	0.05 (p=0.715)	0.212 (p=0.0295)
Keys				0.083 (p=0.465)	0.245 (p=0.0114)
None					0.162 (p=0.101)
Return Label					

First, it is relevant to note that all drive appearances experienced some degree of success in convincing participants to pick them up and plug them into their computers. The one statistically significant difference between drive labels can be found between drives that contained a return label and confidential, exams, and keys drives. The return label-none comparison is not statistically significant ($p = 0.101$), but is close to significance at the 0.1 level. We suspect that this difference is because participants often opened files on the flash drives in order to locate their owners, a hypothesis that is

supported in our analysis of the survey responses and our discussions with people who returned the drives to us. The presence of a return label with an email address allowed participants to contact the owner without needing to plug the flash drive in and open any files.

Drop Time

As mentioned previously, we dropped drives during two time periods: the morning (6-10am) and the afternoon (1-5pm). The morning time period was designed to catch the attention of participants who were going to work or for lunch, while the afternoon time period was designed to catch the attention of participants who were leaving work. The difference between the two periods is shown in Table 3.3.

Table 3.3: Opens by time period. While both times of day appear to be effective, the morning appears to be slightly more so.

Time Period	Dropped	Opened	Fraction Opened
Afternoon	148	64	0.43
Morning	149	71	0.48

These two groups are not statistically significantly different (test of equal proportions, $p = 0.518$). We believe that this difference does not exist because our analysis of checking the drives suggests that people pick up drives relatively quickly when they see them.

Drop Day

We dropped the majority of the flash drives on Monday and Tuesday. We exclude 48 drives (corresponding to six different locations) from this analysis; these drives were deferred until Wednesday because the researchers were unable to place the drives during the desired time intervals on previous days. In this section, we analyze the proportion of opens based on the originally scheduled drop day. Due to an error in the experimental setup, keys and unlabeled drives were dropped on Monday, while confidential and return label drives were dropped on Tuesday; originally, all types of drives were to be dropped on each day. Exam-labeled drives were dropped on both days.

Out of 125 drives dropped on Monday, 67 were opened for an open fraction of 0.54. Out of 124 drives dropped on Tuesday, 51 were opened for an open fraction of 0.41. There is a statistically significant difference between the two groups of flash drives (test of equal proportions, p = 0.065) at the 0.1 level. However, if we remove the return label drives from the data set, the two groups are no longer statistically significantly different (test of equal proportions, p = 0.476). This change suggests that the presence of the return label drives on Tuesday is primarily responsible for the differences between drop days.

Location

As mentioned previously in this paper, we divided the flash drives among 30 different locations in 5 different categories. The fraction of drives opened in each category is shown in Table 3.4, while the fraction of drives opened by location is shown in Table 3.5. The difference-of-proportions comparisons of categories can be found in Table 3.6.

Table 3.4: Opens by location category. Parking lots are the most effective category and academic rooms are the least.

Location Category	Total	Opened	Fraction Opened
Academic Room	58	25	0.43
Common Room	60	26	0.43
Hallway	59	24	0.41
Outside	60	28	0.47
Parking Lot	60	32	0.53

Note that there are no statistically significant differences between location types when we consider all flash drives. However, parking lots appear to be the most effective vector, with Lot A3, Lot C9, and Lot F28's high positions in the location rankings primarily influencing the result.

We also note a few interesting subgroups and analyze them here.

- 6-Pack Lobby and PAR Main Room are dorms on the University of Illinois campus. Combined, students opened 16 of the 20 drives dropped there, for an open fraction of 0.80.
- Grainger Library and UGL are libraries on the University of Illinois

Table 3.5: Opens by location. Individual location appears to strongly influence open rate.

Rank	Location	Total	Opened	Fraction Opened
1	PAR Main Room	10	9	0.90
2	6-Pack Lobby	10	7	0.70
2	Lot A3	10	7	0.70
2	Lot C9	10	7	0.70
2	Near CSL	10	7	0.70
6	Bardeen Quad	10	6	0.60
6	Lot B21	10	6	0.60
6	Lot F28	10	6	0.60
6	Newmark Civil Engineering Building	10	6	0.60
6	Roger Adams Lab	10	6	0.60
11	Altgeld	10	5	0.50
11	Foellinger Auditorium	10	5	0.50
11	Grainger Library	10	5	0.50
11	Law Building Lecture Hall	10	5	0.50
11	Near ARC	10	5	0.50
11	South Quad	10	5	0.50
11	UGL	10	5	0.50
18	Beckman Cafe	10	3	0.30
18	Engineering Hall	10	3	0.30
18	Grainger Auditorium (ECEB)	10	3	0.30
18	Illini Union Food Court	10	3	0.30
18	Lot D22	10	3	0.30
18	Lot E2	10	3	0.30
18	Main Quad Paths	10	3	0.30
18	MEB/MEL	10	3	0.30
18	Natural Resources Building	10	3	0.30
27	BIF Lecture Hall	8	2	0.25
28	South of Krannert	10	2	0.20
28	Inside CRCE	5	1	0.20
30	David Kinley Hall	9	1	0.11
31	CRCE Lobby	5	0	0.00

Table 3.6: Differences in open fraction by location category. The ParkingLot/Hallway comparison has the highest magnitude. None of these differences are significant at the 0.1 level.

	AcademicRoom	CommonRoom	Hallway	Outside	ParkingLot
AcademicRoom		-0.002 (p=1)	0.024 (p=0.937)	-0.036 (p=0.838)	-0.102 (p=0.354)
CommonRoom			0.027 (p=0.914)	-0.033 (p=0.854)	-0.1 (p=0.361)
Hallway				-0.06 (p=0.636)	-0.127 (p=0.23)
Outside					-0.067 (p=0.584)
ParkingLot					

campus. Combined, students opened 10 of the 20 drives dropped there, for an open fraction of 0.50.

- Beckman Cafe and Illini Union Food Court are public eating places on the University of Illinois campus. Combined, students opened 6 of the 20 drives dropped there, for an open fraction of 0.30.

- Bardeen Quad, Main Quad Paths, and South Quad are centrally located quads for the north, main, and south portions of campus, respectively. Combined, students opened 14 out of the 30 drives dropped there, for an open fraction of 0.47.

- CRCE Lobby and Inside CRCE are the publicly accessible lobby and card-swipe accessible lobbies for one of the University of Illinois recreation centers. Students only opened 1 of the 10 drives dropped there, for an open fraction of 0.1.

The dorms are the most interesting of these subgroups due to their significant effectiveness. We offer two explanations for this: first, we expect more students transit through these locations because they are living spaces. Second, at the University of Illinois, freshmen are required to stay in dorms. As such, the populations of these areas are likely to trend younger and thus are likely to be less aware of this sort of attack.

We also briefly mention the ineffectiveness of CRCE Lobby: this lobby is observed by a front desk that is continually staffed for the times of day that the experiment ran. We thus suspect that front desk personnel confiscated our flash drives soon after we dropped them.

Finally, we provide a geographic analysis of this data. When we selected our 30 locations, we divided them into three groups of using two east-west streets on the University of Illinois campus. "North" describes the northernmost, followed by "Main" and then "South." These divisions are geographically significant for the University of Illinois because north campus houses most of the engineering program along with associated research labs; the main and south campuses host other majors. Open fractions by geographic region type are shown in Table 3.7 and differences between these groups are shown in Table 3.8.

Interestingly, the University of Illinois north campus has the highest open rate, although the differences between it and other campuses are not sta-

Table 3.7: Opens by location geography. The north quad appears to be the most effective location.

Campus	Total	Opened	Fraction Opened
main	100	40	0.40
north	100	49	0.49
south	97	46	0.47

Table 3.8: Difference-of-proportions p-values by location geography. None of these differences were significant at the 0.1 level.

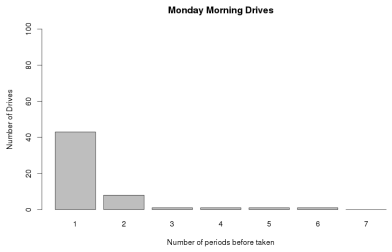
	main	north	south
main		-0.09 (p=0.255)	-0.074 (p=0.365)
north			0.016 (p=0.937)
south			

tistically significant. We posit two explanations for this result: first, the north campus is more geographically compact. Additionally, two studies in our related work [34, 38] found that computer expertise was positively correlated with malware compromise. As many engineering buildings are on north campus and as engineers tend to be more likely to be computer experts, it is possible that the differences we see here serve as a (weak) proxy for computer expertise.

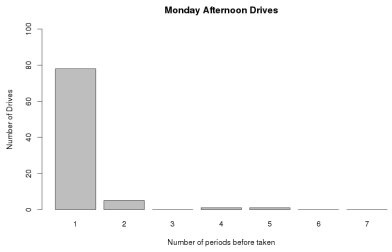
3.3.4 Observed Drop Status

Researchers were also instructed to monitor the drive status after the drives were dropped and report whether the drive had been found, not found, or moved. In this section, we consider the number of periods before the drive was taken. Note that we are omitting drives that were marked as "moved" from this dataset and consider the remaining 284 drives in our analysis. The dataset was split into 4 groups based on drop time; however, these groups do not contain the same number of drives with Monday morning and Tuesday afternoon containing 55 and 58 drives, and Monday afternoon and Tuesday morning containing 85 and 86 drives. The results are shown in Table 3.9 and Figure 3.5.

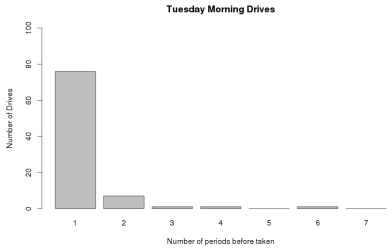
The most noticeable trend in the data is that the majority of drives were taken within the first period after being dropped. This was largely expected as traffic during the day period is extremely high and drives were very visible.



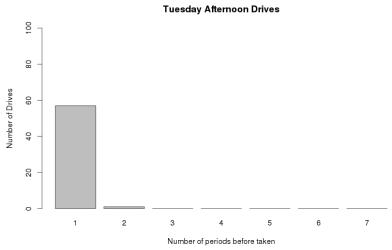
(a) Lag times for Monday morning drives until they were picked up.



(b) Lag times for Monday afternoon drives until they were picked up.



(c) Lag times for Tuesday morning drives until they were picked up.



(d) Lag times for Tuesday afternoon drives until they were picked up.

Figure 3.5: Periods before a drive was marked as taken by original drop time. All drop times show similar distributions.

Furthermore, many drives were expected to be picked up by janitorial staff during the night period. It is interesting that the drives dropped off during night periods were almost all picked up within the first period. This most likely due to the fact that drives that were not picked up by passersby were picked up by cleaning staff.

Table 3.9: Periods before a drive was marked as taken. Researchers checked on drives twice a day during normal drop times. The range of hours corresponding to the possible time difference between the drop and the taken update is also shown. Drives were picked up quickly.

Number of periods	Number of hours	Monday Morning	Monday Afternoon	Tuesday Morning	Tuesday Afternoon
1	3-21	43	78	76	57
2	20-28	8	5	7	1
3	27-45	1	0	1	0
4	44-52	1	1	1	0
5	51-69	1	1	0	0
6	68-76	1	0	1	0

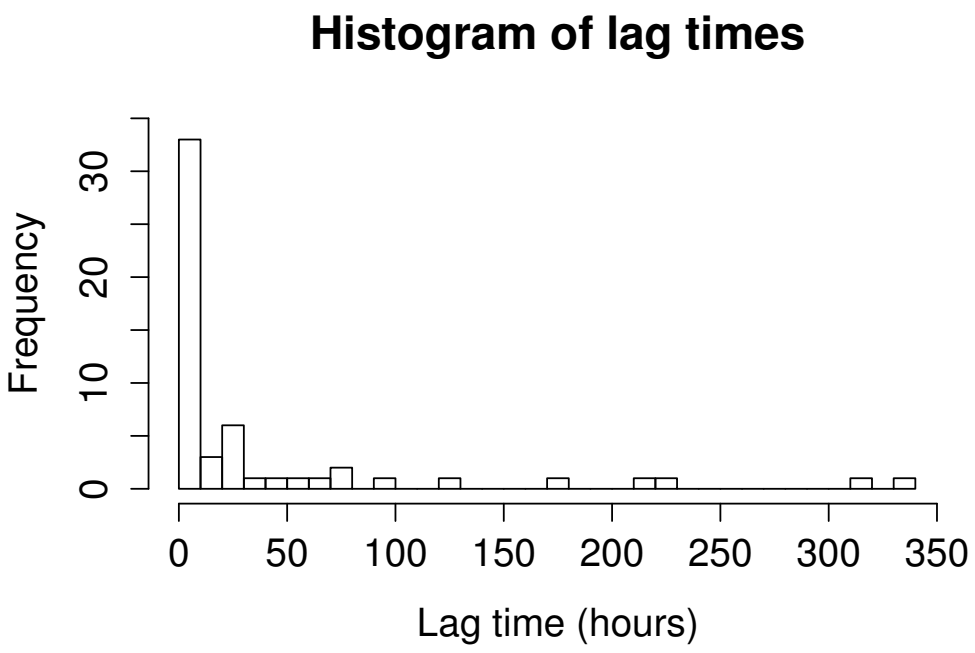


Figure 3.6: Time between drop and first open for all consented drives. This distribution shows that most drives are opened soon after they are dropped, although a long tail exists.

3.3.5 Measured Lag Times

As our central server records the timestamps when it receives a message indicating a drop or a file open, we are also able to provide statistics about the precise time between when a drive is dropped and opened. However, we only provide this statistic (abbreviated as lag time for this section) for participants who consented to provide their data.

Out of the 298 dropped flash drives, 56 people opened a file on the flash drives and gave us permission to use their data in our study. Two participants who consented to the use of their data but did not open a file (likely from opening the HTML file in a virtual machine and then manually following the consent link) were excluded from this analysis. One drive that was opened before it was dropped (due to a technical error on the researchers' part) was also excluded from the analysis. A histogram of lag times can be found in Figure 3.6. Thirty-five participants opened the drive within the first 12 hours of it being dropped; 44 opened a drive within 48 hours.

The median time it took for someone to open a flash drive was 6.933 hours,

with the average time being 38.480 hours.

Table 3.10 shows the average and median lag times when separated between the day and time the drive was dropped.

Table 3.10: The average and median time (in hours) between when the flash drive was dropped and opened, grouped by original drop time. Mornings showed a smaller median lag than afternoons did.

Day	Median	Average
Monday Morning	1.812	34.820
Monday Afternoon	7.776	44.45
Tuesday Morning	2.130	50.740
Tuesday Afternoon	8.651	27.446

Lag time demonstrated a long tail, similar to the drop status data.

The mornings tended to have a far smaller lag time than the afternoons. We suspect that this is because participants who picked up drives in the mornings were on their way to work or school and were going to use a computer sooner than participants in the afternoon were.

3.3.6 Opened Files

In this section, we briefly analyze the files that were opened by participants who consented to share their data. Table 3.11 shows which files participants in the experiment opened first.

Note that unlabeled drives along with drives containing keys and return labels all have similar personal folder contents, consisting of the three top-level folders "Documents," "Pictures," and "Math Notes." As such, three times as many drives had this folder structure. Confidential drives contained the "employee," "strategy," and "2015_proj1" folders, while exam drives contained folders designed to replicate semester numbers.

We notice a few interesting trends in this data. First, the personal file designed to replicate a resume ("/Documents/resume.pdf.html") is the most frequently opened file, with 14 opens. This adds support to the hypothesis that many participants desired to return the drive to its owner; resumes often contain contact information. However, the second-most-opened file on personal drives is a picture file that is the first (in lexicographic order) in the Pictures folder. As contact information is not frequently found in image files,

Table 3.11: Files that were opened first by participants in the experiments. A few files represent the majority of opens.

File Name	Frequency
/Documents/resume.pdf.html	14
/Pictures/Winter Break/0101150001.jpg.html	10
/sp15/examA.pdf.html	6
/2015_proj1/feb12proposalA.pptx.html	4
/2015_proj1/patent_app_0217.pdf.html	3
/fa10/examA.pdf.html	3
/Documents/reflective_essay_02.docx.html	2
/employee/termination_notice_4317_05_17_2015.pdf.html	2
/Math Notes/2-13.docx.html	2
/strategy/plan_for_2015_2016.pptx.html	2
No file recorded	2
/employee/termination_notice_4318_05_17_2015.pdf.html	1
/fa10/solutionsA.pdf.html	1
/fa13/examB.pdf.html	1
/Pictures/Winter Break/1224142256.jpg.html	1
/Pictures/Winter Break/1226141505.jpg.html	1
/Pictures/Winter Break/1231142359.jpg.html	1
/sp10/examA.pdf.html	1
/strategy/0425_meeting_notes.pdf.html	1

we suspect that subjects may have chosen this file out of curiosity. However, we emphasize that these files were placed in three times as many drives as the confidential and exam drive files.

For exam drives, the most popular choice is "/sp15/examA.pdf.html". This file is the first in a folder that refers to the semester in which the experiment was conducted; as the experiment occurred during the last regular week of classes, it is perhaps unsurprising that students looked to see if current final exams could be found on the drive.

For confidential drives, both of the files in the 2015_proj1 folder are the most popular. We suspect that this popularity is due to the fact that the 2015_proj1 folder is first in a lexicographic ordering of folder names and because both files appear to contain information that could identify the owner.

Finally, we note that two drives recorded consent without file opens; this suggests to us that the HTML files were opened in text editors (or virtual machines without internet connections) and the link to consent was manually followed. This result is interesting because it suggests that some users are indeed practicing increased security hygiene around the files.

In Table 3.12, we show the frequencies of the number of times files were opened for consenting participants.

Table 3.12: Frequency of the number of file opens. Most people open only one or two files, although some participants opened many.

Number of Files Opened	Frequency
0	2
1	17
2	15
3	7
4	6
5	3
6	3
10	2
11	2
23	1

Note that the majority of participants only opened one or two files. This is unsurprising, as the purpose of the experiment is made clear with the first file open and all files have (visibly) identical contents. We suspect that additional file opens beyond the first were primarily motivated by curiosity

about the other contents of the drive by participants, although we did detect one case of abuse where participants were repeatedly filling out surveys for additional compensation.

3.3.7 Operating System

In this section, we analyze aggregate data about the operating system (pulled from the user agent string that was sent to our central server upon file open) of the computers on which files were opened. Table 3.13 shows the total number of drives opened by operating system. Note that some user-agent strings contained incomplete data, giving results such as "Windows" or "Linux" rather than a specific version. We provide the data in this form, and suggest specific versions that these are likely to correspond to.

Table 3.13: Number of file opens by operating system. Windows 7 was the most prevalent operating system.

Operating System	Number of Opens	Proportion of Opens
Windows 7	32	0.55
Mac OS X	16	0.28
Windows	4	0.07
Linux	3	0.05
None	2	0.03
Ubuntu	1	0.02

Aggregate data pulled from W3Counter [55] suggests that the Windows category could likely be either Windows 8, or Windows XP.

Aggregates by type of operating system are shown in Table 3.14.

Table 3.14: Number of file opens by operating system family. Windows machines were the most prevalent.

Operating System Family	Number of Opens	Proportion of Opens
Linux	4	0.07
Mac	16	0.28
Windows	36	0.63
None	2	0.03

For comparison, data about the total population of operating systems (pulled from user-agent strings, again from W3Counter) are shown in Table 3.15. Note that we normalize this data by removing Android and iOS

use percentages from the calculation (24.04% in aggregate) and re-calculate proportions; we do so because most Android and all iOS devices lack full-sized USB ports to plug flash drives into and thus are not representative of computers that were used in our study.

Table 3.15: Proportion of operating systems in the general web-browsing population.

Operating System Family	Proportion of Opens
Linux	.03
Mac	.08
Windows	.79

The proportion of Mac users in this experiment is significantly (Fisher's exact test, $p = 3.128 \cdot 10^{-5}$) greater than the proportion of Mac users seen in the W3Counter data, and the proportion of Windows users (Fisher's exact test, $p = 0.0046$) is significantly lower in our data set. To apply Fisher's exact test, we multiplied the proportion by 1000 and used this number in calculations (i.e., Linux was represented as the proportion 33 out of 1000). We speculate that this could be due to demographic purchasing habits; college students may own more Macs than the general population.

3.3.8 Browser

In this section, we analyze the reported browser for each opened (consented) flash drive. Note that "Other" refers to an unknown browser in our user-agent parser, rather than a browser that does not fit into the above categories. The number of flash drive opens by browser are shown in Table 3.16.

Table 3.16: Number and proportion of opens by browser. Note the large number of opens by the 'Other' browser.

Browser	Number of Opens	Proportion of Opens
Chrome	26	0.45
Firefox	12	0.21
IE	8	0.14
Other	6	0.10
Safari	4	0.07
None	2	0.03

For comparison, general-population browsing data from W3Counter is shown in Table 3.17.

Table 3.17: Proportion of web browsers in the general web-browsing population.

Browser	Proportion of Opens
Chrome	0.43
Firefox	0.15
IE	0.17
Safari	0.15
Opera	0.03

None of these browser proportions differ significantly between our data and the W3 data, although Opera is not explicitly found in our data. However, the Other browser user-agent that we collected could belong to any real browser; as such, this comparison is limited in strength.

3.3.9 Summary

In summary, we find that the time and date at which flash drives were dropped, as well as the category of the drop location or its placement on campus do not significantly impact open rates. However, flash drives that do not contain return labels tend to be significantly more effective than those that do. Individual locations show a significant amount of variation in effectiveness. Most drives are picked up quickly, and individuals tended to gravitate to a few different files on the drives. Participants' computers tend to be Macs significantly more frequently than the general population, but their web browser usage is not significantly different than the general population.

Overall, our total open rate (135/297, or 45.45%) is less than the experiments run by Stasiukonis [11] (15/20 = 75%), Wright [12] (32/54 = 59.26%), and McQueen [13] (34/50 = 68%). However, this attack was more effective than the one described in Jacobs [14] (22/60 = 36.66%). Applying the test for equality of proportions, our open rate is significantly less than Stasiukonis's ($p = 0.020$), Wright's ($p = 0.085$), and McQueen's ($p = 0.005$), but not significantly more than Jacobs' ($p = 0.268$). We posit that our attacks were less effective than those in other studies because we targeted a larger

population in more locations; as a result, we chose some locations that were ineffective, reducing our average open rate.

CHAPTER 4

USB SURVEY

In this chapter, we present the methodology and results of the survey that was offered to participants who picked up a flash drive and inserted it into a computer. We also discuss reactions to the experiment from social media and provide analysis about USB flash drives that were returned to the research team. The matter in this chapter is designed to provide an answer to our second research question:

- Why do people pick up the flash drives?

4.1 Survey Methodology

4.1.1 USB Survey

In this survey, participants were asked questions from the SeBIS [8] and the risk taking version of the 30-question DOSPERT [9], as well as demographic questions about their sex, age, highest level of education and employment status. All of the demographic questions were sourced from SurveyMonkey's question bank feature, which provides methodologically sound wording and answer choices [56]. Participants were also asked to indicate their affiliation with the University of Illinois and whether they had heard any information about the study before they had picked up a drive; the latter question was used to filter out data from participants who knew that the experiment was occurring from the analysis. Participants were then asked open-ended questions about how the appearance of the drive influenced them to pick it up, as well as why the users ultimately picked up the drives and clicked on files. We also asked participants how much time they spent on the Internet in a week because other studies (such as [32]) tested to see if this was a factor

that predicted malware compromise. We also include the computer expertise question from Lévesque et al.'s study [34] because computer expertise was found to correlate with compromise in that study. Finally, to track whether participants were paying attention to the survey, we added six attention check questions to the SeBIS and DOSPERT scales; these questions instructed participants to choose a particular answer (e.g., "Please choose often for this item to show you are paying attention.").

The instrument given to participants can be found in Appendix A.

Data for this survey was collected anonymously via the SurveyMonkey online platform [57]. Participants had the option of providing their email addresses if they wished to receive an Amazon electronic gift card or meeting the researchers at a fixed location at a fixed time to receive cash compensation.

4.1.2 Amazon Mechanical Turk Survey

In order to determine whether participants who picked up the flash drives had risk attitudes that varied significantly from the general population, we first wanted to measure the risk attitudes of the general population using an online survey.

This survey was identical to the USB survey, except that the USB-related questions were replaced with questions that asked participants if they had experienced each of five forms of technology-related compromise within the past two years. These forms (e-mail or social networking compromise, malware infection, data loss, data theft, and unauthorized credit card purchases) were chosen to represent a varied subset of cybercrime victimization.

However, we did not have time to perform this experiment by the time of this publication. Instead, we use Blais and Weber's [9] and Egelman and Peer's [8] work as baselines to compare against in our analysis in Section 4.2.

4.2 Survey Results

In this section, we discuss the results of the survey that was administered to participants who picked up and plugged in the flash drives.

We received 80 survey responses. After discarding 7 incomplete responses, 1 response in which the participant self-identified as under 18 years of age, and 1 response in which the participant self-identified as knowing about the study, we see 71 responses. We explicitly note that this number is larger than the 58 flash drives in the experiment associated with explicit participant consent.

To check to see whether this difference was due to intentional action on participants' behalf, we analyzed the timestamps created when a file was opened on a drive and when a survey was started in SurveyMonkey. We associated a survey with a particular flash drive if we recorded a flash drive open between zero and five minutes before the survey was started. When we performed this association, we found that 11 survey responses were associated with a single flash drive; we suspect that this was an attempt to earn additional compensation using the flash drive. To correct for this pattern, we included the first response associated with the drive and removed the other 10 responses from our dataset.

As two responses out of the original 80 were removed due to prior experience and age considerations, and as two drives were associated with no opened files, our difference then becomes potentially as large as 71 - 10 - 58 + 2 + 2 = 7 responses. However, we believe that this worst-case margin of error is acceptable given the possibility that multiple participants could have recorded their experiences with a single flash drive in other cases. As such, we analyzed 61 survey responses for the demographic portions of the analysis. In the case of the DOSPERT and SEBIS data, we also removed participants who answered "prefer not to answer" on any question on the relevant scale. This reduced our sample size to 56 for the DOSPERT and 58 for the SeBIS.

While 3 respondents failed 1 out of 6 attention-check questions, our IRB did not specify attention-check questions as exclusion criteria for this data and we do not feel that these failures are significant.

4.2.1 Open-Ended Questions

In this section, we discuss trends that we found in open-ended responses to survey data.

We note the following trends:

- **Participants underestimate the threat of infected websites.** Multiple participants indicated that they perceived clicking on the files as relatively safe because the files had the HTML extension. To quote one participant, when asked whether they had any concerns about opening the file on the flash drive: "At first I did, however after seeing how the flash drive had only files on it which were directing to a website (.html link)I wasn't as worried as I have Antivirus and spyware software installed on my computer." This suggests that participants are less aware of possible web-based threats than malicious executables.

- **Participants view shared resources as a proxy for safe computing.** Multiple participants indicated that they opened the flash drive on a university shared machine instead of their own machine to mitigate the risk of causing problems for their own computers. Upon being asked whether they had any concerns about plugging in the flash drive, one respondent answered: "I would have, so I sacrificed a university computer." This finding seems to suggest that participants view computers they may not own or administer as devices that can be used to test unknown objects.

- **Some participants have strong security hygiene.** A small number of respondents indicated that they took significant protective measures. Some opened the HTML file using a text editor, and others attached the flash drives to machines that did not have internet access. This is an encouraging result, as this sort of response is an effective way to deal with this sort of threat.

- **Users generally trust security software to protect their computers.** A few respondents indicated that they did not worry about the risk of malware infection because of the software setup of their machines. This occasionally extended to operating systems as well: "I trust my Macbook to be a good defense against viruses."

- **Curiosity and desire to return the flash drive dominate motivations.** The majority of participants indicated that they investigated the flash drive to return it to its proper owner and were searching for

Table 4.1: Survey respondents by sex. They do not differ as a whole from the Illinois student population.

Sex	Frequency	Fraction	p
Male	35	0.65	0.21
Female	18	0.33	0.13
Prefer not to answer	1	0.02	

contact information on the drive. Many participants highlighted the presence of keys as a factor that helped them to pick up the drive: "It placed more urgency to return it to its owner. Someone could be locked out of their apartment/house or something, so I would rather return it faster." A smaller fraction indicated that they wished to view the contents of the drive. This curiosity appears to dominate over suspicion at times; multiple participants indicated that they believed the drives labeled "Final Exam Solutions" and "Confidential" were intentionally dropped (e.g., "At no point did I consider that it was a USB of test questions... either way, I have to know what is on it."), but were still willing to investigate. More concerningly, this extended to opening a file on the drive: "I was wondering why a jpeg picture had an html address." Two participants also admitted to picking up the drives because they needed another flash drive for storing assignments.

4.2.2 Demographics

In this section, we analyze the responses to demographic questions posed in the survey.

Sex

Table 4.1 shows the proportion of participants by self-identified sex. We excluded 7 staff members from this analysis.

This does not statistically significantly differ from the University of Illinois's student population, which has 24163 men, 19436 women, and 3 unknown persons for a total of 43603 students [58] (test of equality of proportions, $p = 0.21$ for men and $p = 0.13$ for women).

Table 4.2: Survey respondents by age. The significant majority of students were of either underclassman undergraduate age (18-20) or in their twenties.

AgeGroup	Frequency	Fraction	p
18-20	19	0.35	0.76
21-29	32	0.59	0.63
30-39	1	0.02	0.37
40 or older	2	0.04	0.12
Prefer not to answer	0	0.00	

Age

Table 4.2 shows the proportion of participants by age. We removed seven participants (two in the 21-29 range, three in the 30-39 range, and two in the 40-49 range) who self-identified as staff.

Note that most participants reported as either 18-20 or 21-29. As typical undergraduates in the United States range from 18-23 in age and many graduate students are in their 20s, this result makes sense given the affiliation data in Section 4.2.2.

We also compare these fractions with those found in the University of Illinois's demographic data [58]. As this data provides year of birth, we estimate that birthdays are evenly distributed across days. As May 1 is approximately 1/3 into the year, we assign 1/3 of birthdays to one age and 2/3 to the next (e.g., 1/3 of the people born in 1992 are 23 and the rest are 22). Using this estimate, we find that 16623/43603 (38.1%) students are in the 18-20 age group, 24025 (55.1%) students are in the 21-29 age group, 2402 (5.5% students are in the 30-39 age group, and 473 (1.1%) are 40 or older. Applying the test for equal proportions to this data, we find that the fraction of 18-20 year olds does not significantly differ ($p = 0.76$) and the fraction of 21-29 year olds does not significantly differ ($p = 0.63$) between the University population and participants in our study. Using Fisher's exact test, we find that the fraction of 30-39 year olds does not significantly differ between these populations ($p = 0.37$), as well as the fraction of participants over 40 ($p = 0.12$).

We believe that our sample is mostly representative of the University of Illinois's student population at large.

Table 4.3: Survey respondents by affiliation to the University of Illinois. Few faculty and staff participated in the study.

Affiliation	Frequency	Fraction	p
Faculty	0	0.00	0.08
Staff	7	0.11	0.53
Graduate Student	13	0.21	0.94
Undergraduate Student	40	0.66	0.39
None	0	0.00	
Prefer not to answer	1	0.02	

Table 4.4: Affiliation populations at the University of Illinois.

Affiliation	Frequency	Fraction
Faculty	2974	0.0542
Staff	8314	0.1515
Graduate Student	11024	0.2008
Undergraduate Student	32579	0.5935

Affiliation

The affiliations of participants to the University of Illinois are shown in Table 4.3.

Most participants were undergraduate students and no participants self-reported as faculty. This data matches the age findings, which suggest that survey participants tended to be young and relatively inexperienced in their studies.

For faculty and staff numbers for comparison purposes, we refer to the University of Illinois's facts page [59]. The numbers for undergraduate enrollment (32,579) and graduate enrollment (11,024) match the ones given in our other source [58]. As there are 2,974 faculty at the University of Illinois as well as 8,314 staff, our entire population is 54,891. We show these numbers in Table 4.4.

Applying the test for equal proportions, we find that the proportions of undergraduate students ($p = 0.39$), graduate students ($p = 0.94$) and staff ($p = 0.53$) do not significantly differ from the general campus population. Applying Fisher's exact test, we find that significantly fewer faculty ($p = 0.08$) were found in our sample. However, we do note that one participant declined to provide their affiliation.

Table 4.5: Survey respondents by internet usage. Participants spent varying amounts of time on the internet.

Time on Internet	Frequency	Fraction
Less than 10 hours	3	0.05
More than 10 but less than 30 hours	21	0.34
More than 30 but less than 50 hours	27	0.44
More than 50 but less than 80 hours	7	0.11
More than 80 hours	3	0.05
Prefer not to answer	0	0.00

Internet Usage

We asked participants to estimate the amount of time they spent on the internet in a week. This question was included in our survey because other studies (such as Bossler and Holt [32] and Lévesque et al. [34]) include it as a potential predictor using the argument that more internet exposure increased a subject's potential for victimization. The results are shown in Table 4.5.

Participants were approximately equally divided between occasional (10-30 hours a week) and frequent (30-50 hours a week) groups. We are unsure whether both of these groups were popular due to question phrasing, a difference in work habits (such as major), or some other reason. However, it is interesting to note that participants belonged to every possible category, which suggests that this attack works across a broad cross section of internet users.

We do not provide any comparisons to other work in this section because other literature used different question phrasing and did not report statistics about the answer to questions of this form.

Computer Expertise

In order to estimate participants' computer expertise, we asked them a question originally posed in Lévesque et al.'s study [34]. Participants were asked to indicate which (if any) of three computing activities they had previously completed. The responses for this question are shown in Table 4.6 and Table 4.7.

Many participants had participated in multiple computer expertise-related activities. The majority of participants had installed or re-installed an op-

Table 4.6: Survey respondents by computer expertise activity. The majority of participants had participated in operating system installation at some point, and network configuration and web page development were also relatively popular.

Activity	Frequency	Fraction
I have installed or re-installed an operating system on a computer	40	0.66
I have configured a home network	27	0.44
I have created a web page	28	0.46
None of the above	15	0.25
Prefer not to answer	0	0.00

Table 4.7: Survey respondents by number of computer expertise activities performed. About a third of participants could be classified as computer experts in this study.

Number of Activities Performed	Frequency	Fraction
0	15	0.25
1	15	0.25
2	13	0.21
3	18	0.30

erating system at some point in time, and over 40% of participants had completed the other two specified activities.

Approximately 30% of participants completed all three activities, which would define them as experts as described in Lévesque et al. [34]. This ratio is not significantly different than the 18% of participants who were experts given in Lévesque et al. [34]. (Test for equal proportions, $p = 0.24$.)

4.2.3 DOSPERT

In this section, we analyze participant responses to the risk taking scale of the 30-question DOSPERT; this scale is described in further detail in Blais and Weber [9].

Table 4.8 describes the mean, standard deviation, and Cronbach's alpha [60], which is a measure of a scale's reliability, for each domain in both Blais and Weber's paper [9] (for the given English-speaking population) and our study. Data from Blais and Weber [9] is given the subscript "paper," while our data is given the subscript "study.' We also report the results of Welch's two-sample unpaired t-test between each domain in [9] and our paper (e.g., the comparison between the Ethical domain in [9] and the results for our

ethical domain).

Table 4.8: Mean, standard deviation, Cronbach's alpha, and t-test results between domains for the DOSPERT in both Blais and Weber's paper [9] and our study. Participants in our study reported less willingness to try risky activities in all domains except recreational risk.

Domain	M_{paper}	SD_{paper}	α_{paper}	M_{study}	SD_{study}	α_{study}	t	df	p
Ethical	17.97	7.16	0.75	12.59	4.68	0.52	6.48	143.96	1.34E-09
Financial	20.67	8.51	0.83	15.27	5.26	0.67	5.65	153.11	7.62E-08
Health/Safety	21.80	7.84	0.71	19.18	7.06	0.65	2.35	102.66	2.09E-02
Recreational	23.01	9.40	0.86	25.46	10.13	0.87	-1.60	87.91	1.13E-01
Social	32.42	6.44	0.79	29.75	5.67	0.54	2.96	105.00	3.82E-03

It is interesting to note that participants in this study reported significantly smaller scores on all DOSPERT domains except the Recreational domain versus Blais and Weber [9]; this suggests that they are less willing to try risky activities. However, it is important to note that the context of the experiment may have primed participants to be more risk-averse; participants were directed to this survey after they had picked up a flash drive, plugged it in, and been notified that their behavior constitutes a security risk.

4.2.4 SeBIS

In this section, we present participants' responses to the Security Behavior Intentions Scale (SeBIS); this scale is described in further detail in [8].

Table 4.9 describes the mean, standard deviation, and Cronbach's alpha for each of the items in the SeBIS in both Egelman and Peer [8] and our study. We also report the results of Welch's two-sample unpaired t-test between each item in Egelman and Peer [8] and our paper. Table 4.10 describes the mean and standard deviation for each of the subscales in the SeBIS for our study, as well as Cronbach's alpha for both our study and Egelman and Peer [8].

First, we note that Cronbach's alpha for each subscale, shown in Table 4.10, is relatively similar. The main difference in Cronbach's alpha can be found in password generation, which is less in our study.

While many of the item responses in our study have significantly different means than Egelman and Peer's, we choose to focus on the responses that display the greatest differences and comment on their implications. These

Table 4.9: Information about responses to items in the SeBIS in both Egelman and Peer's study [8] and our own. The response items for this scale were {Never (1), Rarely (2), Sometimes (3), Often (4), Always (5)}. We recoded reverse-scored items (indicated by the ^{r} superscript), as in Egelman and Peer's paper. Our averages differ in the case of many questions.

Question	M_{paper}	SD_{paper}	M_{study}	SD_{study}	t	df	p
I set my computer screen to automatically lock if I don't use it for a prolonged period of time.	3.20	1.56	3.93	1.43	-3.66	73.77	4.69E-04
I use a password/passcode to unlock my laptop or tablet.	3.78	1.52	4.17	1.43	-1.97	72.93	5.31E-02
I manually lock my computer screen when I step away from it.	2.63	1.34	3.31	1.52	-3.26	67.67	1.77E-03
I use a PIN or passcode to unlock my mobile phone.	3.21	1.73	3.72	1.68	-2.19	71.75	3.14E-02
I do not change my passwords, unless I have to.	2.65	1.09	1.90	1.00	5.36	73.55	9.07E-07
I use different passwords for different accounts that I have.	3.75	1.04	3.17	1.16	3.64	68.05	5.32E-04
When I create a new online account, I try to use a password that goes beyond the site's minimum requirements.	3.31	1.10	3.41	1.20	-0.63	68.49	5.31E-01
I do not include special characters in my password if it's not required.	3.30	1.29	2.81	1.46	2.45	67.82	1.68E-02
When someone sends me a link, I open it without first verifying where it goes.	4.01	1.01	2.97	1.21	6.30	66.56	2.66E-08
I know what website I'm visiting based on its look and feel, rather than by looking at the URL bar.	3.17	1.08	3.03	1.01	0.96	72.95	3.39E-01
I submit information to websites without first verifying that it will be sent securely (e.g., SSL, https://, a lock icon).	3.69	1.10	3.29	1.16	2.49	69.59	1.52E-02
When browsing websites, I mouseover links to see where they go, before clicking them.	3.69	1.03	3.26	1.37	2.32	64.63	2.34E-02
If I discover a security problem, I continue what I was doing because I assume someone else will fix it.	4.08	0.98	3.71	1.12	2.42	67.35	1.80E-02
When I'm prompted about a software update, I install it right away.	3.07	1.03	2.81	1.02	1.84	71.41	7.03E-02
I try to make sure that the programs I use are up-to-date.	3.78	0.89	3.50	0.92	2.20	69.88	3.14E-02
I verify that my anti-virus software has been regularly updating itself.	3.55	1.23	3.33	1.37	1.18	68.07	2.41E-01

Table 4.10: Subscale means and standard deviations in our study, along with Cronbach's alpha for both studies. All subscale reliabilities except the Password Generation subscale appear to be similar to Egelman and Peer's work [8], confirming that their scale is generally reliable.

Subscale	M_{study}	SD_{study}	α_{study}	α_{paper}
All	52.14	10.34	0.803	0.801
Device Securement	15.04	4.60	0.728	0.764
Password Generation	11.36	3.17	0.503	0.728
Proactive Awareness	16.14	3.92	0.694	0.668
Updating	9.61	2.42	0.554	0.719

differences are unsurprising, as Egelman and Peer's work deals with an Amazon Mechanical Turk sample, while our work deals with a sample of university students and other people affiliated with the university.

Participants guarded their computers more closely. Participants reported they were significantly more likely to manually lock their computers or set their computers to automatically lock when leaving their computers.

Participants trust links more. They were significantly more likely to indicate that they would open a link without first verifying where the link went.

Participants used weaker passwords. They were significantly more likely to reuse passwords and significantly more likely to avoid changing their passwords.

In summary, it appears that participants appear to be more concerned with the physical safety of their computers rather than the strength of their passwords or the validity of the links they follow. In the context of this study, this difference is particularly ironic.

4.3 Reactions to the Experiment

In this section, we examine the public reaction to this study.

The debriefing page found in the HTML files on the flash drives contained contact information for one of the researchers. As a result, we were contacted by various departments who wanted to return the devices. We collected 54 drives; one drive had all of its data formatted, so we could not match it to an existing record and removed it from our analysis.

4.3.1 Returned Drives by Category

Flash Drive Label

While all flash drive labels experienced some degree of success in convincing participants to pick them up and plug them into their computers, it is also relevant to note how the flash drive labels influenced participants to return or attempt to return the drives.

Table 4.11: Returned drives by flash drive label. Drives that contained keys (Keys and Return Label drives) were returned more frequently.

Label	Dropped	Opened	Returned	Fraction Opened	Fraction Returned
Keys	60	29	17	0.48	0.28
Return Label	59	14	11	0.24	0.19
Exams	60	29	11	0.48	0.18
Confidential	58	29	8	0.50	0.14
None	60	27	6	0.45	0.10

From Table 4.11, we see that the keys served as the label with the highest return fraction of 0.28. A likely explanation for this is that keys are viewed as an essential item that many people rely on a daily basis. Since keys are viewed by many as a universally dependent item, the sight of dropped keys may invoke an additional degree of empathy in the participant that the other labels cannot.

Additionally, we can see that for drives with a return, exams, and confidential label, the return fractions were 0.19, 0.18, and 0.14 respectively. Although these return fractions are lower than for the keys, the close range may be explained with similar rationale. The return, exams, and confidential label may be perceived as more valuable to the participant, and therefore it may be worth the altruistic effort required to attempt to return the drive.

The assessment that the perceived value of the label increases the chance of the drive being returned may be further explained by the lower return fraction of .10 for the drives without any label. The lack of the label may make the drive appear like a generic lost flash drive; without any additional perceivable value, the flash drive alone may not be enough to motivate the participant to make an effort to return the drive.

Return Location

Drives that were returned to the same location in which they were scheduled to be dropped are shown in Table 4.12.

We note that certain locations are very effective at returning drives; we hypothesize that this is a per-building policy.

Table 4.12: Returned drives by location. The top four return locations returned the majority of the drives.

Location	Total	Opened	Returned	Fraction Opened	Fraction Returned
David Kinley Hall	9	1	7	0.11	0.78
Newmark Civil Engineering Building	10	6	7	0.60	0.70
Grainger Library	10	5	6	0.50	0.60
Natural Resources Building	10	3	6	0.30	0.60
MEB/MEL	10	3	5	0.30	0.50
Altgeld	10	5	4	0.50	0.40
Bardeen Quad	10	5	4	0.50	0.40
Lot A3	10	7	3	0.70	0.30
Grainger Auditorium (ECEB)	10	3	3	0.30	0.30
CRCE Lobby	5	0	1	0.00	0.20
Near CSL	10	7	2	0.70	0.20
Foellinger Auditorium	10	3	1	0.30	0.10
Lot E2	10	2	1	0.20	0.10
Main Quad Paths	10	3	1	0.30	0.10

Table 4.13: Returned drives that were returned to different locations. Half of the returned drives (28/56) were returned in a different location than they were dropped.

Schedule Location	Return Location	Frequency
Grainger Auditorium (ECEB)	Engineering IT-North Campus	3
Grainger Library	Engineering IT-South Campus	3
MEB/MEL	Engineering IT-North Campus	3
Grainger Library	University Libraries	2
Lot A3	Talbot	2
Bardeen Quad	Engineering IT-South Campus	1
Bardeen Quad	Talbot	1
Bardeen Quad	University Libraries	1
Bardeen Quad	Unknown	1
CRCE Lobby	Altgeld	1
Foellinger Auditorium	Altgeld	1
Grainger Library	Unknown	1
Lot A3	University Libraries	1
Lot E2	Temple Hoyne Buell Hall	1
Main Quad Paths	CSL	1
MEB/MEL	Unknown	1
Near CSL	CSL	1
Near CSL	Engineering IT-North Campus	1
South Quad	Mumford Hall	1
South Quad	Temple Hoyne Buell Hall	1

Different Return Location

Table 4.13 describes location pairs when the return location is different than the scheduled location. It appears that some buildings forward their drives onto different lost and founds, while drives dropped on certain other outside paths are distributed into nearby buildings.

Return Contact

Table 4.14 describes the categories of people who returned the flash drives.

Table 4.14: Returned drives by return contact. Most drives were returned by administrators.

Contact	Returned
Admin	32
Facilities	1
Grad Student	0
IT	18
Professor	1
Student	1

The majority of these contacts were driven by administrative personnel; in discussions with these participants, we learned that many of them served (officially or unofficially) as the contact person for lost items in their individual departments.

4.3.2 E-Mail Contacts

Drives that had return labels attached to them also contained contact information for a fictitious individual. We created 10 such profiles; 5 of the profiles contained male names and 5 of the profiles contained female names. Each name was chosen at random using one of the top 100 most popular first names in the state of Illinois in 1993 and one of the top 100 most popular last names in the United States in the 2000 census [61, 62]. Each person was also given a gmail account of the form "first.last.NNNN@gmail.com", where NNNN represents a four-digit random number selected by the researchers. Only the name and email address were written on the return tag. As we had

10 e-mail accounts and 60 different return label USB keys, we attached each name to 6 different tags.

The number of responses to each fake contact are shown in Table 4.15.

Table 4.15: Emails sent to return return label flash drives after a week in the experiment. All emails were contacted by at least three separate people.

Name	Email	Number of Emails Received	Number of Unique Senders
Trevor Mitchell	trevor.mitchell.5427@gmail.com	7	6
Jared Hill	jared.hill.7589@gmail.com	5	5
Keith Reed	keith.reed.1010@gmail.com	4	4
Jose Gutierrez	jose.gutierrez.4501@gmail.com	5	4
Antonio Diaz	antonio.diaz.4365@gmail.com	3	3
Katherine Hall	katherine.hall.3293@gmail.com	8	6
Brooke Green	brooke.green.1290@gmail.com	4	4
Crystal Roberts	crystal.roberts.2221@gmail.com	3	3
Alexis Peterson	alexis.peterson.5150@gmail.com	6	6
Emma Cruz	emma.cruz.7842@gmail.com	3	3

On average, each recipient had received 4.8 emails from 4.4 different email addresses by one week after the start of the experiment. This average holds for both male and female names, as both the male and female names received a total of 24 different emails from 22 different email addresses. As we only dropped 6 different flash drives with each email address, we consider this result especially encouraging.

4.3.3 Social Media Response

During the experiment, we monitored a few social media sites for descriptions of the experiment. We include this information as an anecdotal proxy for how fast information spread during the duration of the study. The University of Illinois has a sub-forum on the popular user-submitted content site Reddit, entitled r/uiuc. r/uiuc is not university-affiliated; it has 10,565 subscribers and describes events in the university and the cities of Urbana and Champaign. We also monitored the "Free and For Sale" Facebook group for the University of Illinois; this group is also not affiliated with the university and has 10,721 members. Both of these pages are open (i.e., they do not require approval to join). None of the members of the research team posted on either page on posts relating to the study.

On Tuesday, April 28, at 10:52 AM, a student posted a picture of one of the devices with keys in Free and For Sale and identified that the drive was found outside the civil engineering building. We also realized that the same

individual posted in an open group for the Civil Engineering department on the same day at 12:27 AM, indicating that the flash drive in question had been retrieved at some point on Monday.

By Tuesday, April 28, at 1:03 PM, a user on r/uiuc posted after finding drives of various types in multiple locations. The user indicated that they had reported the issue to campus IT and believed that the drives could be part of a research study. Commenters primarily confirmed the presence (and non-maliciousness) of the flash drives and speculated about the purpose of the study. Two users warned readers to avoid plugging the devices into their computers.

By Thursday, April 30, at 10:17 AM, one of the researchers' Facebook friends posted a status indicating that they had noticed multiple USB drives labeled "Confidential" being deliberately left in the building.

By Thursday, April 30, at 4:03 PM, another user (who identified as working for campus IT) posted about flash drives labelled "Final Exam Answers." The author referenced the previous post and encouraged readers not to plug the drives in. Commenters referenced the previous thread, speculated about the purpose of the experiment, and discussed the deletion of the previous post.

Given this evidence, we highlight the following trends in public social media perception of the experiment:

1. **Information spreads using multiple avenues.** While there was relatively little public discussion of the experiment in either reddit post (9 comments in the first and 17 in the second), posters indicated that they had discussed their findings with others and were aware that the drives could be part of an experiment.

2. **The density of the experiment may have been too high.** The creator of the first reddit post indicated that they had found multiple drives in various locations over the course of Monday and Tuesday. While the research team had hoped to reduce the density of the drives to the point where a student would not encounter multiple drives during the course of the experiment, this goal appears to have been missed to a degree.

3. **There may still be a significant lag before drives are identified**

as suspicious. All social media posts that we were able to identify as related to the experiment were found on Tuesday; while the campus population may have been growing increasingly suspicious of the drives before this period, they did not publicly communicate until then. This trend seems to indicate that a motivated attacker may be able to successfully accomplish their objective before a coordinated defense is mounted by the community.

4.3.4 Altruistic Experiences

Twice during the experiment, researchers were given back flash drives that they attempted to drop. The subjects who returned the drives were non-confrontational; we consider these incidents an effective display of altruism that underscores the conclusions of this thesis.

CHAPTER 5

CONCLUSION

5.1 Discussion

This section discusses trends we have noticed in this thesis.

This attack is effective by default. By placing flash drives in locations that are in plain sight, researchers were able to successfully achieve a 45.45% pickup rate. Also, please note that this attack rate is conservative; we only tracked when a participant plugged in a drive and opened a file. Given the fact that all of the drives had disappeared within 3 days of dropping, we believe that some fraction of the remaining population plugged in drives but did not click on files. In practice, this means that the vulnerability rate for the population is even higher.

While we did not find any particular choice of experimental parameters that was significantly superior to all others, we suggest that the following parameters may affect experimental success:

- **Uniqueness is key.** Participants in this experiment began to get suspicious when they noticed multiple flash drives with identical appearances around campus. An "effective" attack in more realistic circumstances involves the victims being unaware that they are being compromised. As our data suggests that the appearance of the flash drive does not significantly impact pickup rates (provided that it does not have a return label), we believe that randomizing the appearances of drives would help to avoid general detection.

- **Both attacks and detection can be quick, but coordinated response can be delayed.** Most activations occurred within a day of the drop; however, discussions with staff who returned drives suggested that the drives were brought to their attention within a short time as

well. While individual departments may have been made aware of the incident rather quickly, coordinated responses (by both students and IT staff) to address the drives took approximately a day to materialize. This suggests that a window of opportunity exists for an attacker to compromise an organization before a coordinated response to the threat is mounted. However, we suspect that corporate environments (with centralized IT departments and better-trained users) would be able to handle this attack more quickly than universities (with less centralization and less-experienced users).

- **Proper location selection is key.** Location was the one parameter that appeared to vary the most in effectiveness within the experimental design. While our sample size for each location is not large enough to make significant conclusions about the data set, it seems to be the case that a properly chosen location can make the difference in the effectiveness of an attack. We also note that one report to engineering IT staff was made from the department level; a poorly chosen target can raise an alarm about the attack.

- **Participants appear to be generally motivated by altruism and curiosity.** Participants returned 54 drives (that the research team is aware of) to administrative staff and IT security personnel. They tended to open files that could be expected to contain contact information ("resume.pdf.html"), and typically emailed the owners of flash drives without snooping whenever possible. In our survey, they typically expressed a desire to return the flash drives to their proper owners.

However, some fraction of participants expressed in the survey that they explored the contents of the flash drives because they were curious. They also opened files that should have corresponded to images or exam solutions for the current semester, neither of which typically locate the owner. (However, we do concede that exams at the University of Illinois often specify the professor's name on a cover sheet for the exam; while we do not believe it is likely, it is possible that students may be using the current exam to attempt to return the drive to its proper owner. This idea is supported by the fact that files corresponding to the exam were opened, rather than solutions.) Interestingly, it appears that some of this curiosity was actually caused by

suspicion about the experiment.

Our evidence appears to suggest that these two sources appear to be the primary drivers of the effectiveness of this experiment.

Finally, we discuss the conclusions with regards to our hypotheses:

- Hypothesis 1: Participants will place the flash drives in computers and click on the relevant files. **Supported** by our data.

- Hypothesis 2a: Participants who pick up flash drives will primarily report doing so for two reasons: to return the flash drive to its owner (an altruistic reason) and out of curiosity/to benefit from the contents of the drive (a self-interested reason). **Supported in a weak sense** by our data; altruism and curiosity (although not explicit self-interest) appear to motivate participants, although we do not know the role of other potential motivators that we did not test for.

- Hypothesis 2b: Psychological scales that measure risk attitude will correlate with cybercrime victimization in the general population because participants who believe that picking up the flash drive is too risky will not do so and will thus not be victimized. **Unknown** because we did not have time to run the experiment.

- Hypothesis 2c: Participants who picked up the flash drives will have greater risk attitude scores than the general population. **Not supported** by the data; in comparison with the population given in one of Blais and Weber's papers [9], participants who picked up the flash drives displayed significantly less willingness to participate in risky activities in all domains except the recreational domain.

- Hypothesis 3a: The time of day at which drives are placed will not significantly impact success rates because people will quickly pick up the drives once they are dropped. **Supported** by the data.

- Hypothesis 3b: The type of location at which drives are dropped will significantly impact success rates because different location types will attract different demographics and will have different drive visibilities. **Suggested** by the data, although we do not have a large enough number of samples to conclude comfortably and we do not know participants' demographics on a per-location basis.

- Hypothesis 3c: Altruistically configured drives will have a greater success rate than drives designed to motivate self-interest because participants will be more motivated to plug in the drive if they believe they can help someone by doing so. **Not supported** by the data; in fact, return label drives performed significantly worse. However, many participants expressed altruistic motivations in the survey.

- Hypothesis 3d: Both altruistically configured and self-interest-configured drives will have greater success rates than the control group. **Not supported** by the data; unlabeled drives performed similarly to all other groups (except return label drives).

5.2 Methodological Limitations

We include this section by describing limitations of the current study in order to properly contextualize its contributions. The following limitations are described from most serious to least serious, according to our judgment.

Only a few drives were dropped in each location. While our results suggest that location could be a predictor of compromise, only 10 drives were dropped in each location; this number is small enough to limit the conclusions that we can draw from location data. We believe that this limitation is inherent to this type of study, as a larger number of drives in any given location may have aroused further suspicion.

Participants were aware of the experiment by mid-day Tuesday. Due to posts to the Facebook Lost and Found group as well as Reddit, word of the flash drives was publicized to an audience measuring in the thousands. We believe that our quick placement of the drives (over a two-day period) may have increased suspicion; however, by the time that the Reddit post went up, we had dropped $\frac{3}{4}$ of the drives and were in the process dropping the rest. We believe that this limitation is inherent to this type of study, as we needed to drop a significant number of drives in order to collect enough samples to perform statistical tests.

Some drives were dropped on different days. Drives dropped in CRCE Lobby and Inside CRCE tended to accumulate over time; the small size of this space necessitated that we drop some of these drives on a later

day. Due to a mix-up involving automated directions in the Android app, drives placed in Lot B21 and Lot D22 were temporarily swapped; researchers retrieved the drives and placed them the next day. One drive was accidentally marked as dropped in Law Building Lecture Hall, although the drive was not dropped. It was properly dropped the next day. BIF Lecture Hall was generally locked during drop times, so drops were put off until the room was unlocked again. In each case, drives were dropped during the same time period in which they were scheduled.

As such, we believe that these late drops only affect data analysis involving the evolution of the experiment over the course of days; we excluded these locations from the appropriate analyses as a result.

5.3 Future Work

In this section, we discuss ideas and questions that could be explored more thoroughly in future work.

Do participants behave differently after the study? Other work [48] suggests that users behave differently after they have been subjected to a "security incident." It would be interesting to monitor individual users for a period of time after the experiment to see if their security posture changes significantly. If we promote awareness of the attack or administer the study again, will users recognize the attack and warn others, or will they fall victim again?

How does word of the attack spread organically? While we were able to detect a few alert posts related to the experiment, we suspect that we were unable to measure a significant amount of discussion regarding the flash drives. It would be interesting to measure the propagation of information about the experiment as it occurred.

Can this attack be coordinated? The framework that we built for this experiment allows us to program many flash drives in a relatively short amount of time; it took the research team approximately 12 hours to program and precisely categorize 300 drives, for a time of approximately 2.4 minutes per drive. Given the relatively scalable nature of our software (and the relative lack of bookkeeping necessary for a real attack), we believe it would be possible to half this programming time. At a rate of 500 drives per day,

a motivated attacker could program 7000 drives in two weeks' time. As our app can be run on common Android smartphones and as the drives are the only other physical component of the attack, we believe it would be possible for an attacker to distribute the attack across multiple locations by shipping pre-programmed drives to other agents in other locations and coordinating the app via the central server.

5.4 Conclusion

The purpose of this paper was to provide insight into the classic security anecdote: will a handful of dropped flash drives in the parking lot of a company effectively compromise it?

Our study, in which we dropped 297 flash drives around campus of the University of Illinois, suggests yes. By measuring many different dropped drive parameters, we were able to provide some introductory insight into the effectiveness of different drive combinations. By monitoring lag times between drop and pickup and drop and file open, we were able to confirm the rapidity of the experiment. By picking up returned drives, we were able to quantify the return of drives through various channels and provide more information supporting our altruism hypothesis. By analyzing user agent strings of browsers who accessed our servers, we were able to gain insight into victims' systems. By monitoring social media and e-mails to our fake accounts, we were able to confirm the community's mass response and interest in returning the drives to their proper owners. Finally, by asking users about their experiences with the experiment, we were able to gain valuable insight into their thought process.

We were able to learn that the attack is generally effective and that participants appeared to be primarily interested in returning the drives to their original owners, although they also displayed some curiosity.

APPENDIX A

SURVEY INSTRUMENT

Tables A.1 and A.2 contain the instrument that was offered to participants who picked up a flash drive and placed it into their computers.

Table A.1: The survey given to respondents who picked up USB flash drives (part 1).

SeBIS: [Never (1), Rarely (2), Sometimes (3), Often (4), Always (5), Prefer not to answer]
1. I set my computer screen to automatically lock if I don‘t use it for a prolonged period of time. 2. I use a password/passcode to unlock my laptop or tablet. 3. I manually lock my computer screen when I step away from it. 4. I use a PIN or passcode to unlock my mobile phone. 5. I do not change my passwords, unless I have to. 6. Please choose often for this item to show you are paying attention. 7. I use different passwords for different accounts that I have. 8. When I create a new online account, I try to use a password that goes beyond the site‘s minimum requirements. 9. I do not include special characters in my password if it‘s not required. 10. When someone sends me a link, I open it without first verifying where it goes. 11. I know what website I‘m visiting based on its look and feel, rather than by looking at the URL bar. 12. I submit information to websites without first verifying that it will be sent securely (e.g., SSL, https://, a lock icon). 13. When browsing websites, I mouseover links to see where they go, before clicking them. 14. If I discover a security problem, I continue what I was doing because I assume someone else will fix it. 15. When I‘m prompted about a software update, I install it right away. 16. I try to make sure that the programs I use are up-to-date. 17. Select always as the answer to this question. 18. I verify that my anti-virus software has been regularly updating itself.
DOSPERT (2006): For each of the following statements, please indicate the likelihood that you would engage in the described activity or behavior if you were to find yourself in that situation. Provide a rating from Extremely Unlikely to Extremely Likely, using the following scale: [Extremely Unlikely (1), Moderately Unlikely (2), Somewhat Unlikely (3), Not Sure (4), Somewhat Likely (5), Moderately Likely (6), Extremely Likely (7), Prefer not to answer]
1. Admitting that your tastes are different from those of a friend. 2. Going camping in the wilderness. 3. Betting a day‘s income at the horse races. 4. Investing 10% of your annual income in a moderate growth diversified fund. 5. Select the third bubble from the left for this item. 6. Drinking heavily at a social function. 7. Taking some questionable deductions on your income tax return. 8. Disagreeing with an authority figure on a major issue. 9. Betting a day‘s income at a high-stake poker game. 10. Having an affair with a married man/woman. 11. If 2+2 = 5, please choose extremely likely. Otherwise, choose extremely unlikely. 12. Passing off somebody else‘s work as your own. 13. Going down a ski run that is beyond your ability. 14. Investing 5% of your annual income in a very speculative stock. 15. Going whitewater rafting at high water in the spring. 16. Betting a day‘s income on the outcome of a sporting event. 17. Engaging in unprotected sex. 18. Revealing a friend‘s secret to someone else. 19. Driving a car without wearing a seat belt. 20. Investing 10% of your annual income in a new business venture. 21. Taking a skydiving class. 22. Purchasing a banana for $1000. Choose extremely unlikely if you wouldn‘t. 23. Riding a motorcycle without a helmet. 24. Choosing a career that you truly enjoy over a more secure one. 25. Speaking your mind about an unpopular issue in a meeting at work. 26. Select not sure as the answer to this question. 27. Sunbathing without sunscreen. 28. Bungee jumping off a tall bridge. 29. Piloting a small plane. 30. Walking home alone at night in an unsafe area of town. 31. Moving to a city far away from your extended family. 32. Starting a new career in your mid-thirties. 33. Leaving your young children alone at home while running an errand. 34. Not returning a wallet you found that contains $200.

Table A.2: The survey given to respondents who picked up USB flash drives (part 2).

Demographics:
1. Are you male or female? [Female, Male, Prefer not to answer] 2. What is your age? [17 or younger, 18-20, 21-29, 30-39, 40-49, 50-59, 60 or older, Prefer not to answer] 3. What is the highest level of school you have completed or the highest degree you have received? [Less than high school degree, High school degree or equivalent (e.g., GED), Some college but no degree, Associate degree, Bachelor degree, Graduate degree, Prefer not to answer] 4. Which of the following categories best describes your employment status? [Employed, working full-time; Employed, working part-time; Not employed, looking for work; Not employed, NOT looking for work; Retired; Disabled, not able to work; Prefer not to answer]
Other questions:
1. On average, how much time did you spend on the Internet per week (e.g., searching for information, checking email, streaming videos)? [Less than 10 hours, More than 10 but less than 30 hours, More than 30 but less than 50 hours, More than 50 but less than 80 hours, More than 80 hours, Prefer not to answer] 2. Select the task(s) that you have previously accomplished; if none of these tasks applies to your situation, then please select "None of the above": [I have installed or re-installed an operating system on a computer, I have configured a home network, I have created a web page, None of the above, Prefer not to answer]
USB Questions:
1. Why did you pick up the flash drive and insert it into your computer? [Open-ended] 2. Why did you open a file on the flash drive? [Open-ended] 3. Did you happen to notice any of the following things about the flash drive you picked up? [It had a label attached to it, It had items (such as keys) attached to it, Other (please specify), Prefer not to answer] 4. Did any labels attached to the flash drive significantly impact your decision to pick it up and place it into your computer? [Yes, No, I did not notice any labels attached to the flash drive, Prefer not to answer] 5. (If yes to 4) How did any labels attached to the flash drive influence you to pick it up and insert it into your computer? [Open-ended] 6. Did any items (such as keys) attached to the flash drive significantly impact your decision to pick it up and place it into your computer? [Yes, No, I did not notice any items attached to the flash drive, Prefer not to answer] 7. (If yes to 6) How did items (such as keys) attached to the flash drive influence you to pick it up and insert it into your computer? [Open-ended] 8. Did you have any concerns about picking up the flash drive and inserting it into your computer? If so, please explain. [Open-ended] 9. Did you have any concerns about opening the file on the flash drive? [Open-ended] 10. Did you take any precautions before opening the file on the flash drive (e.g., scanning it for viruses)? [Open-ended] 11. Had you heard any information about this research study in the past? [Yes, No, Prefer not to answer] 12. Please select your affiliation with the University of Illinois, if any. [Faculty, Staff, Graduate Student, Undergraduate Student, No affiliation, Prefer not to answer]

REFERENCES

[1] Codenomicon, "The Heartbleed Bug," 2014. [Online]. Available: http://heartbleed.com

[2] J. Geffner, "VENOM: Virtualized Environment Neglected Operations Manipulation," 2015. [Online]. Available: http://venom.crowdstrike.com/

[3] US-CERT, "Alert (TA14-268A): GNU Bourne-Again Shell (Bash) Shellshock Vulnerability," US-CERT, Tech. Rep., 2014. [Online]. Available: https://www.us-cert.gov/ncas/alerts/TA14-268A

[4] M. J. Schwartz, "Social engineering attacks cost companies," *Dark Reading*, 2001. [Online]. Available: http://www.darkreading.com/vulnerabilities-and-threats/social-engineering-attacks-cost-companies/d/d-id/1100278?

[5] Ponemon Institute, "2013 Cost of Cyber Crime Study: United States," Ponemon Institute, Tech. Rep., 2013. [Online]. Available: http://media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_13455.pdf

[6] K. Zetter, "An unprecedented look at Stuxnet, the worlds first digital weapon," *Wired*, 2014. [Online]. Available: http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

[7] Security Research Labs, "Turning USB peripherals into BadUSB," Tech. Rep., 2014. [Online]. Available: https://srlabs.de/badusb/

[8] S. Egelman and E. Peer, "Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS)," in *SIGCHI Conference on Human Factors in Computing Systems (CHI '15)*. ACM, 2015. [Online]. Available: http://dl.acm.org/citation.cfm?id=2702249

[9] A.-R. Blais and E. U. Weber, "A domain-specific risk-taking (DOSPERT) scale for adult populations," *Judgment and Decision Making*, vol. 1, no. 1, 2006.

[10] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information Security Policy Compliance: An Empirical Study of Rationality-based Beliefs and Information Security Awareness," *MIS Q.*, vol. 34, no. 3, pp. 523–548, Sep. 2010. [Online]. Available: http://portal.acm.org/citation.cfm?id=2017477

[11] S. Stasiukonis, "Social engineering, the USB way," *Dark Reading*.

[12] S. Wright, "Honey stick project - phase 1 results," Streetwise Security Zone, Tech. Rep., 2012. [Online]. Available: http://www.streetwise-security-zone.com/members/streetwise/adminpages/HSP-Phase1-Results

[13] M. McQueen, "Software and human vulnerabilities," in *ARC World Industry Forum 2010*, Feb. 2010.

[14] J. R. Jacobs, "Measuring the effectiveness of the USB flash drive as a vector for social engineering attacks on commercial and residential computer systems," M.S. thesis, Embry-Riddle Aeronautical University, 2011.

[15] T. N. Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer, "Social Phishing," *Commun. ACM*, vol. 50, no. 10, pp. 94–100, Oct. 2007. [Online]. Available: http://dx.doi.org/10.1145/1290958.1290968

[16] M. Huber, S. Kowalski, M. Nohlberg, and S. Tjoa, "Towards Automating Social Engineering Using Social Networking Sites," in *International Conference on Computational Science and Engineering, 2009. CSE '09.*, vol. 3. IEEE, Aug. 2009. [Online]. Available: http://dx.doi.org/10.1109/cse.2009.205 pp. 117–124.

[17] L. Carettoni, C. Merloni, and S. Zanero, "Studying Bluetooth Malware Propagation: The BlueBag Project," *Security & Privacy, IEEE*, vol. 5, no. 2, pp. 17–25, Mar. 2007. [Online]. Available: http://dx.doi.org/10.1109/msp.2007.43

[18] S. Wright, "The Symantec smartphone honey stick project," 2012. [Online]. Available: https://www.symantec.com/content/en/us/about/presskits/b-symantec-smartphone-honey-stick-project.en-us.pdf

[19] N. Christin, S. Egelman, T. Vidas, and J. Grossklags, "It's All about the Benjamins: An Empirical Study on Incentivizing Users to Ignore Security Advice," in *Financial Cryptography and Data Security*, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2012, vol. 7035, pp. 16–30. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-27576-0_2

[20] F. L. Greitzer, J. R. Strozer, S. Cohen, A. P. Moore, D. Mundie, and J. Cowley, "Analysis of Unintentional Insider Threats Deriving from Social Engineering Exploits," in *Security and Privacy Workshops (SPW), 2014 IEEE*. IEEE, May 2014. [Online]. Available: http://dx.doi.org/10.1109/spw.2014.39 pp. 236–250.

[21] D. Wagenaar, D. Pavlov, and S. Yannick, "USB baiting," *Universite van Amserdam*, 2011.

[22] S. Milgram, L. Mann, and S. Harter, "The lost-letter technique: A tool of social research," *The Public Opinion Quarterly*, vol. 29, no. 3, pp. pp. 437–438, 1965. [Online]. Available: http://www.jstor.org/stable/2746945

[23] E. Lastdrager, L. Montoya, P. Hartel, and M. Junger, "Applying the Lost-Letter Technique to Assess IT Risk Behaviour," in *Socio-Technical Aspects in Security and Trust (STAST), 2013 Third Workshop on*. IEEE, June 2013. [Online]. Available: http://dx.doi.org/10.1109/stast.2013.15 pp. 2–9.

[24] E. U. Weber, A.-R. Blais, and N. E. Betz, "A domain-specific risk-attitude scale: measuring risk perceptions and risk behaviors," *J. Behav. Decis. Making*, vol. 15, no. 4, pp. 263–290, Oct. 2002. [Online]. Available: http://dx.doi.org/10.1002/bdm.414

[25] T. Buchanan, C. Paine, A. N. Joinson, and U.-D. Reips, "Development of measures of online privacy concern and protection for use on the Internet," *J. Am. Soc. Inf. Sci.*, vol. 58, no. 2, pp. 157–165, Jan. 2007. [Online]. Available: http://dx.doi.org/10.1002/asi.20459

[26] J. Joireman, M. J. Shaffer, D. Balliet, and A. Strathman, "Promotion orientation explains why future-oriented people exercise and eat healthy: evidence from the two-factor consideration of future consequences-14 scale." *Personality & social psychology bulletin*, vol. 38, no. 10, pp. 1272–1287, Oct. 2012. [Online]. Available: http://dx.doi.org/10.1177/0146167212449362

[27] B. Fischhoff, P. Slovic, S. Lichtenstein, S. Read, and B. Combs, "How safe is safe enough? A psychometric study of attitudes towards technological risks and benefits," *Policy Sciences*, vol. 9, no. 2, pp. 127–152, Apr. 1978. [Online]. Available: http://dx.doi.org/10.1007/bf00143739

[28] A. Welsh and J. A. Lavoie, "Risky eBusiness: An examination of risk-taking, online disclosiveness, and cyberstalking victimization," *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 2012.

[29] L. E. Cohen and M. Felson, "Social Change and Crime Rate Trends: A Routine Activity Approach," *American Sociological Review*, vol. 44, no. 4, pp. 588–608, Aug. 1979. [Online]. Available: http://dx.doi.org/10.2307/2094589

[30] B. H. Spitzberg and J. Rhea, "Obsessive Relational Intrusion and Sexual Coercion Victimization," *Journal of Interpersonal Violence*, vol. 14, no. 1, pp. 3–20, Jan. 1999. [Online]. Available: http://dx.doi.org/10.1177/088626099014001001

[31] B. H. Spitzberg, L. Marshall, and W. R. Cupach, "Obsessive relational intrusion, coping, and sexual coercion victimization," *Communication Reports*, vol. 14, no. 1, pp. 19–30, Jan. 2001. [Online]. Available: http://dx.doi.org/10.1080/08934210109367733

[32] A. M. Bossler and T. J. Holt, "On-line activities, guardianship, and malware infection: An examination of routine activities theory," *International Journal of Cyber Criminology*, vol. 3, no. 1, pp. 400–420, 2009.

[33] F. T. Ngo and R. Paternoster, "Cybercrime victimization: An examination of individual and situational level factors," *International Journal of Cyber Criminology*, vol. 5, no. 1, pp. 773–793, 2011.

[34] F. L. Levesque, J. Nsiempba, J. M. Fernandez, S. Chiasson, and A. Somayaji, "A Clinical Study of Risk Factors Related to Malware Infections," in *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, ser. CCS '13. New York, NY, USA: ACM, 2013. [Online]. Available: http://dx.doi.org/10.1145/2508859.2516747 pp. 97–108.

[35] F. L. Levesque, J. M. Fernandez, and A. Somayaji, "Risk prediction of malware victimization based on user behavior," in *Malicious and Unwanted Software: The Americas (MALWARE), 2014 9th International Conference on*. IEEE, Oct. 2014. [Online]. Available: http://dx.doi.org/10.1109/malware.2014.6999412 pp. 128–134.

[36] D. Canali, L. Bilge, and D. Balzarotti, "On the Effectiveness of Risk Prediction Based on Users Browsing Behavior," in *Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security*, ser. ASIA CCS '14. New York, NY, USA: ACM, 2014. [Online]. Available: http://dx.doi.org/10.1145/2590296.2590347 pp. 171–182.

[37] G. Maier, A. Feldmann, V. Paxson, R. Sommer, and M. Vallentin, "An Assessment of Overt Malicious Activity Manifest in Residential Networks," in *Detection of Intrusions and Malware, and Vulnerability Assessment*, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2011, vol. 6739, pp. 144–163. [Online]. Available: http://dx.doi.org/10.1007/978-3-642-22424-9_9

[38] T. F. Yen, V. Heorhiadi, A. Oprea, M. K. Reiter, and A. Juels, "An Epidemiological Study of Malware Encounters in a Large Enterprise," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '14. New York, NY, USA: ACM, 2014. [Online]. Available: http://dx.doi.org/10.1145/2660267.2660330 pp. 1117–1130.

[39] V. Garg and J. Camp, "End User Perception of Online Risk under Uncertainty," in *System Science (HICSS), 2012 45th Hawaii International Conference on*. IEEE, Jan. 2012. [Online]. Available: http://dx.doi.org/10.1109/hicss.2012.245 pp. 3278–3287.

[40] D. LeBlanc and R. Biddle, "Risk perception of internet-related activities," in *Privacy, Security and Trust (PST), 2012 Tenth Annual International Conference on*. IEEE, July 2012. [Online]. Available: http://dx.doi.org/10.1109/pst.2012.6297924 pp. 88–95.

[41] A. P. Felt, S. Egelman, and D. Wagner, "I've Got 99 Problems, but Vibration Ain't One: A Survey of Smartphone Users' Concerns," in *Proceedings of the Second ACM Workshop on Security and Privacy in Smartphones and Mobile Devices*, ser. SPSM '12. New York, NY, USA: ACM, 2012. [Online]. Available: http://dx.doi.org/10.1145/2381934.2381943 pp. 33–44.

[42] E. Chin, A. P. Felt, V. Sekar, and D. Wagner, "Measuring User Confidence in Smartphone Security and Privacy," in *Proceedings of the Eighth Symposium on Usable Privacy and Security*, ser. SOUPS '12. New York, NY, USA: ACM, 2012. [Online]. Available: http://dx.doi.org/10.1145/2335356.2335358

[43] S. Flinn and J. Lumsden, "User Perceptions of Privacy and Security on the Web," pp. 15–26, 2005. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.60.9160

[44] B. Friedman, D. Hurley, D. C. Howe, E. Felten, and H. Nissenbaum, "Users' Conceptions of Web Security: A Comparative Study," in *CHI '02 Extended Abstracts on Human Factors in Computing Systems*, ser. CHI EA '02. New York, NY, USA: ACM, 2002. [Online]. Available: http://dx.doi.org/10.1145/506443.506577 pp. 746–747.

[45] L. Koved, S. Trewin, C. Swart, K. Singh, P.-C. Cheng, and S. Chari, "Perceived security risks in mobile interaction," in *Symposium on Usable Privacy and Security (SOUPS)*, 2013.

[46] K. Onarlioglu, U. O. Yilmaz, E. Kirda, and D. Balzarotti, "Insights into User Behavior in Dealing with Internet Attacks," in *Network and Distributed Systems Security Symposium (NDSS)*, Feb. 2012.

[47] G. R. Milne, L. I. Labrecque, and C. Cromer, "Toward an Understanding of the Online Consumer's Risky Behavior and Protection Practices," *Journal of Consumer Affairs*, vol. 43, no. 3, pp. 449–473, Sep. 2009. [Online]. Available: http://dx.doi.org/10.1111/j.1745-6606.2009.01148.x

[48] A. Vance, B. B. Anderson, C. B. Kirwan, and D. Eargle, "Using Measures of Risk Perception to Predict Information Security Behavior: Insights from Electroencephalography (EEG)," *Journal of the Association for Information Systems*, vol. 15, no. 10, 2014. [Online]. Available: http://aisel.aisnet.org/jais/vol15/iss10/2/

[49] H.-S. Rhee, C. Kim, and Y. U. Ryu, "Self-efficacy in information security: Its influence on end users' information security practice behavior," *Computers & Security*, vol. 28, no. 8, pp. 816–826, Nov. 2009. [Online]. Available: http://dx.doi.org/10.1016/j.cose.2009.05.008

[50] A. Bandura, *Social foundations of thought and action: A social cognitive theory.* Prentice-Hall, Inc, 1986.

[51] Z. Benenson, A. Girard, N. Hintz, and A. Luder, "Susceptibility to URL-based Internet attacks: Facebook vs. email," in *Pervasive Computing and Communications Workshops (PERCOM Workshops), 2014 IEEE International Conference on.* IEEE, Mar. 2014. [Online]. Available: http://dx.doi.org/10.1109/percomw.2014.6815275 pp. 604–609.

[52] G. B. Forbes, TeVault, and H. F. Gromoll, "Regional differences in willingness to help strangers: A field experiment with a new unobtrusive measure," *Social Science Research*, vol. 1, no. 4, pp. 415–419, Dec. 1972. [Online]. Available: http://dx.doi.org/10.1016/0049-089x(72)90086-5

[53] University of Illinois, Urbana-Champaign, "Campus map," 2015. [Online]. Available: http://illinois.edu/map/map.pdf

[54] University of Illinois, Urbana-Champaign, "Parking and regulations," 2015. [Online]. Available: http://www.parking.illinois.edu/parking_items/rules-amp-regulations

[55] W3Counter, "February 2015 market share," Feb. 2015. [Online]. Available: http://www.w3counter.com/globalstats.php?year=2015&month=02

[56] L. Gauthier, "How Question Bank Was Built," 2011. [Online]. Available: https://www.surveymonkey.com/blog/en/blog/2011/07/27/how-question-bank-was-built/

[57] SurveyMonkey, "SurveyMonkey.com," 2015. [Online]. Available: https://www.surveymonkey.com/

[58] Division of Management Information, "On-campus fall 2014 statistical abstract of ten-day enrollment," 2014. [Online]. Available: http://www.dmi.illinois.edu/stuenr/abstracts/fa14_ten.htm

[59] University of Illinois, Urbana-Champaign, "Illinois facts," 2015. [Online]. Available: http://illinois.edu/about/facts.html

[60] L. Cronbach, "Coefficient alpha and the internal structure of tests," *Psychometrika*, vol. 16, no. 3, pp. 297–334, Sep. 1951. [Online]. Available: http://dx.doi.org/10.1007/bf02310555

[61] Social Security Administration, "Popular names by state," 2015. [Online]. Available: http://www.ssa.gov/cgi-bin/namesbystate.cgi

[62] United States Census Bureau, "Frequently occurring surnames from the census 2000," 2014. [Online]. Available: http://www.census.gov/topics/population/genealogy/data/2000_surnames.html